HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

TASK FORCE

The Donald C. Hellmann Task Force Program

Data Security [digital image] *howtostartablogonline.net*

International Cybersecurity: De-escalating tensions in a digital era

2019

Henry M. Jackson School of International Studies
University of Washington, Seattle
Task Force Report Winter 2019

International Cybersecurity:

De-escalating Tensions in a Digital Era

Faculty Advisor
Dr. Jessica Beyer

Evaluator
Bruce McConnell
Executive Vice President of the EastWest Institute

Editors
Victoria O'Laughlin
Sarah Sanguinet

Coordinator
Angelia Miranda

Authors
Amy Champagne
Nick Drainville
Coley Felt
Zhiqin Gao
Connor Herriford
Evan Hobbs
Mardav Jain
Nicola Kalderash
Sara Koeck
Eleanor Krabill
Brooke Manning
Angelia Miranda
Philipp Nonnast
Victoria O'Laughlin
Sarah Sanguinet
Haiyan Wang

Executive Summary

Within the last decade, nation-states and their populations have experienced an exponential rise in cyberattacks against critical infrastructure. Cyberattacks are an attractive addition to traditional warfare for adversaries, as nation-state actors who utilize them can more easily evade attribution. However, cybertactics that target critical infrastructure cause the same grave damage as purely kinetic attacks. Developing international cybersecurity norms encourages a more peaceful and collaborative international sphere, averting cyberattacks before they occur.

This report aims to provide a cohesive understanding of a range of nation-state cyber actor types and preferences, investigating what constitutes the basis of each country's current cyberstrategy and using that as a foundation for understanding each country's stance towards creating international norms. To do this, we conducted 14 country case studies to understand country preferences in negotiations to develop international cybersecurity norms. Across our cases, we find that country preferences are determined by perspectives on international collaboration, national sovereignty, cybercapability development, and political constraints. We also surveyed existing international agreements and conversations, which signify a common willingness to cooperate in shaping international cybersecurity norms.

Drawing from major findings within case studies and the analysis of existing agreements, this report offers six policy recommendations that nation-states can agree upon to establish effective international cybersecurity norms. Our recommendations to the international community are:

1) Involve as many nation-states as possible in drafting international cybersecurity agreements
2) Reaffirm principles from prior agreements
3) Encourage neutral states or non-cyber powers to coordinate agreements
4) Commit to building national cybersecurity capacity, confidence, and trust
5) Encourage informal dialogue between nation-states
6) Acknowledge the increasing threat of cyberattacks

Report Findings

Our survey of current agreements on the principles and norms of cyberspace found that they are increasing in number, but are less than unified in their ideologies. There is also no binding language or mechanisms for holding countries accountable for cyberattacks. More and more countries are pursuing regional and bilateral accords, as well as dialogues on the ideal cybersecurity environment, but factions have appeared.

A key source of disagreement is the extent to which international law strictly applies to cyberspace, or whether new norms and laws should be made that are tailored to cyberspace. There is also a consistent call across agreements for confidence building and capacity building, but little evidence that countries have been working towards this.

The nuances seen within past attempts at forming international cybersecurity agreements indicate low communication, and, therefore, trust, within cyberspace. However, overlapping elements within existing agreements show strong potential for shaping international cybersecurity norms. To move towards this goal, addressing nation-states' different sociopolitical arenas must be prioritized to accommodate all preferences and circumstances.

Case Studies

Fourteen country case studies were examined to form a holistic overview of different nation-state cybersecurity positions and strategies. The report groups countries together based on common major offensive actors, additional major actors, swing states, Paris Call signatories, and victim states to clarify each country's position in the cyber realm.

In each of the 14 case studies, background context is provided for understanding the country's international cybersecurity status. Each case study then discusses major adversarial actors and their pattern of attacks. Researchers also evaluated each country's national cybersecurity strategy, including offensive attacks and policy landscape to understand the domestic elements producing a country's stance on internet governance. The case studies conclude by assessing the country's likelihood of collaborating with other nation-states to shape international cybersecurity norms.

Case Findings

The cases demonstrate a consensus among nation-states that cyberattacks threaten global peace. International acknowledgement of increasing cyberwarfare threats can be inferred by the numerous existing bilateral agreements that address cybersecurity policy development. To combat increasing cyberthreats internationally, national approaches to solving cybersecurity issues were compared across cases. This report found that many countries' domestic sociopolitical context and

cybersecurity positions can be applied to the international discussion about shaping international cybersecurity norms.

International Collaboration

The case studies within this report demonstrate a common theme of nation-states seeking international collaboration and wanting to remain actively involved in shaping international cybersecurity norms. Some countries have shown a preference to encourage collaboration among governments, others advocate specifically for expertise and information sharing, and some simply favor inclusion at international meetings.

Specifically, Saudi Arabia expresses their wish to see more collaboration among international governments. The country hopes to obtain this goal through capacity-building and international conversation. Although Canada and Saudi Arabia's preferences about international internet governance are very different, they that government collaboration is favorable. Similarly, Ukraine and Iran advocate for cooperation and expertise sharing.

Ukraine stresses that the lack of international agreements to support international cooperation is problematic, signifying a willingness to collaborate. Iran prefers information sharing between organizations, as their CERT is openly talking to other CERTs to communicate current and past viruses to remain up-to-date in international cybersecurity incidents.

Another country that advocates for international collaboration is Brazil, as the country's long history with external interference motivates the country to embrace inclusion and a voice for all. For example, the Budapest Convention of Cybercrime emerged from the Council of Europe, excluding non-European countries from input and attendance. Brazil refrained from ratifying the Convention, simply because the country was not present in its creation. This emphasizes the significance of full international inclusion at international debates.

National Sovereignty

Countries that strongly prefer national internet sovereignty such as Russia and China have differing levels of flexibility in terms of shaping international cybersecurity norms and their preferences must also be accommodated. Countries in this category generally prefer internet control, minimal outside influence, and opt-out clauses in the case of a treaty conflicting with sovereignty.

Russia, for example, is in this category because of its highly-sovereign political preferences, including heavy data localization and minimal collaboration with international corporations. Russia will not agree to any policy that infringes on these ideas. Its desire for more control over the internet creates a barrier to shaping international cybersecurity norms, as Russia is a major offensive actor in cyberspace

and would ideally be included in international meetings and debates. While the country has sovereignty reservations, opt-out clauses can allow for leeway in international cybersecurity policymaking.

Advancing Offensive and Defensive Capabilities

Another overarching theme across our country case studies is capacity development. This development includes strengthening defensive capabilities, such as the creation of CERTs and media literacy education programs, as well as offensive capabilities, such as the stockpiling of vulnerabilities.

Saudi Arabia values commitment to focusing on the defensive cyberstrategy. During international debates, Saudi Arabia tends to focus on combating the use of cyberweapons, partially due to its experience as victim of Iranian cyberattack on critical infrastructure. In Canada, defensive cybersecurity infrastructure is highly developed. Canada is committed to developing a central national cybersecurity entirety, advancing its cybersecurity policies, strengthening public-private sector collaboration, and educating its population on the prevalence of cyberthreats. To complement its extensive infrastructure, Canada's offensive cyberstrategy is created in anticipation of threats. The Canadian government has passed a bill that encourages the use of offensive, non-violent cyberattacks in the best interest of national security, when necessary. The US also values the use of offensive cyberstrategy, as it is actively stockpiles vulnerabilities for potential cyberwarfare, similar to those used in the infamous Stuxnet attack.

Political Constraints

Throughout our cases, political context greatly influences a country's orientation to cybersecurity issues. Significant geopolitical tension, turbulent history, and ideological conflict are examples of ways in which international politics can sway agreement outcomes.

For instance, Ukraine is likely to reject any idea proposed by Russia, due Russia's annexation of Crimea and ongoing conflict with Ukraine. Similarly, Iran is less likely to cooperate with the United States, given political tension caused in part by Stuxnet—an attack attributed to the US that targeted Iranian nuclear centrifuges—tension that increased with the US's exit from the nuclear deal. Given the substantial influence the US has on both international relations and internet governance, it is likely that any international cybersecurity agreement will need US support.

Policy Recommendations

We evaluated existing multilateral and bilateral agreements and cybersecurity strategy to demonstrate 14 different nation-states' cybersecurity positions and what those nations would agree to or disagree with in relation to international cybersecurity norms. An increasing number of countries are developing cybercapabilities to combat the increasing threat of cyberattacks. Concurrently, there is an active dialogue on potential rules for cyberwarfare, common principles for acting in cyberspace, and the future of international cybersecurity cooperation. These discussions take place in international organizations; bilateral, multilateral, and regional agreements; and informal dialogue between state actors.

In spite of these efforts, there remains no existing binding international agreement on cybersecurity norms. And, to effectively curtail the significant threat of cyberattacks, a set of international norms must be agreed upon. However, the existing international track record has failed to take significant steps towards a comprehensive binding agreement on international cybersecurity norms. Below we discuss the following recommendations to the international community in detail: (1) Involve as many nation-states as possible in drafting international cybersecurity agreements; (2) reaffirm principles from prior agreements; (3) encourage neutral states or non-cyber powers to coordinate agreements; (4) commit to building national cybersecurity capacity, confidence, and trust; (5) encourage informal dialogue between nation-states; and (6) acknowledge the increasing threat of cyberattacks.

Recommendation 1: Involve as Many Nation-States as Possible in Drafting International Cybersecurity Agreements

Being absent during the drafting process of agreements can deter countries from signing. When the Council of Europe drafted the Budapest Convention as non-members, India, China, and Brazil were not involved in the process. These countries subsequently declined to sign and ratify the agreement because they were not present. When creating international cybersecurity policy, including as many actors as possible is crucial to the potential reach and influence agreements can have. Doing so not only adds a more holistic international perspective to agreements, but also counterbalances perceptions that the US and Europe dictate international internet governance.

Including as many nation-states as possible in drafting processes requires consistent international dialogue, inclusive meeting environments, and mandatory attendance at important global policy meetings and debates. Mandatory attendance to policy meetings and debates also requires providing assistance to countries that do not have the resources to attend, in order to ensure their

attendance. These practices can encourage nations to participate in shaping an international cybersecurity policy framework.

Recommendation 2: Reaffirm Principles from Prior Agreements

Developing cohesive international cybersecurity agreements has been a challenging goal for policymakers, given conflicting national perspectives. Restating ideas that have already been formally agreed upon helps to build a basis of alignment when uniting a complex set of actors.

For example, compiling common principles from international cybersecurity agreements—such as the applicability of the UN Charter and the principles of state sovereignty and right to defend to cyberspace—in a comprehensive cybersecurity agreement would be useful in establishing clear common ground between all countries involved. This common ground will aide in forming a foundation to offset the differences in ideology when it comes to cybersecurity norms, such as the ability of government to regulate cyberspace and the role of stakeholders in cybersecurity.

Recommendation 3: Encourage Neutral States or Non-Cyber Powers to Coordinate Agreements

Nation-states may be wary of major powers proposing agreements. In terms of drafting international agreements, remaining cognizant of the nation-state intentions, international power structures, and historical legacies is important in creating fair policy.

Brazil and South Africa are examples of countries who may be wary of more powerful countries such as the US, Russia, and China using their advanced capabilities to dominate and push cybersecurity norms that are not in the best interest of smaller countries. The 2017 UN GGE is a specific instance of talks being derailed due to a smaller country—Cuba—disagreeing with US demands to strictly apply current international law to cyberspace.

Potentially, neutral or small states could coordinate cybersecurity agreements. For instance, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and the Model Nuclear Weapons Convention were both proposed by neutral states. In 1958, Ireland proposed the NPT; Costa Rica and Malaysia proposed the Model Nuclear Weapons Convention in 2007.

Recommendation 4: Commit to Building National Cybersecurity Capacity, Confidence, and Trust

Trust is difficult to obtain without collaboration among states and organizations. The 2014-15 UN GGE Members unanimously agreed that capacity building could protect underdeveloped, vulnerable state infrastructure from malicious actors. Members also agreed that capacity building involves information sharing, as well as effective responses by both developed and developing states. Evidently,

an increase in capacity building would be a major step towards gaining confidence and trust in cyberspace, with the end goal of shaping international cybersecurity norms.

If organizations emulate this and commit to building capacity internationally, public trust in cybersecurity organizations would increase, fulfilling the goals of responding to cyberattacks, mitigating crises, and creating stronger cybersecurity infrastructure. Capacity building would allow countries with underdeveloped capabilities to shift focus from constantly defending themselves from attacks to actively contributing to shaping norms.

In addition, an opt-out clause would accommodate countries who prioritize sovereignty in agreeing to follow at least some elements of these recommendations, enhancing trust and security in cyberspace regardless of partial agreement. The creation of a program modeled on UN Peacekeeping, coordinated by a neutral state, could provide a framework for nation-states to follow.

Recommendation 5: Encourage Informal Dialogue Between Nation-States

An absence of consistent dialogue between nation-states, regarding cybersecurity development expectations and progress of cybersecurity measures, creates a tense atmosphere. Informal checks and balances between nation-states would increase the transparency of national cybersecurity measures, encouraging a more diplomatic environment.

The regional, bilateral, and multilateral agreements that currently exist are a step in the right direction for creating and strengthening international cybersecurity norms. Evidently, the international cybersecurity sphere will greatly benefit from increasing the quantity and quality of these agreements, which may differ depending on signatories' sociopolitical circumstances.

To initiate discussions about shaping international cybersecurity norms, it could be helpful to place existing international frameworks, such as the Non-Proliferation Treaty and the Geneva Protocol, in the context of cybersecurity strategy. Using these frameworks, emulating and applying the rhetoric of prioritizing global safety to cybersecurity, could alleviate seemingly daunting cybersecurity issues and promote international dialogue.

Recommendation 6: Acknowledge the Increasing Threat of Cyberattacks

Acknowledging the increasing urgency to confront the threat of cyberattacks is a major step towards building international security. In the best interest of international security and trust, it is crucial to assert international cybersecurity norms that can accommodate varied nation-state interests.

A way towards achieving this goal is to enforce a regulation condemning substantial, intentional attacks on critical infrastructure. Including a clause regarding mutual non-aggression that would strictly

discourage the first use of cyberweapons would also contribute to combating the proliferation of cyberattacks.

For example, creating an international cybersecurity framework truly based off the Geneva Convention would encourage signatory states to refrain from perpetrating any attacks upon critical infrastructure. Applying the Geneva Convention to cybersecurity would demonstrate the severity of cyberweapons and indirectly demand no first use.

Survey of Existing International Agreements

By Connor Herriford and Angelia Miranda

Table 1: International Agreements Snapshot

Agreements Included in this Report		
International Agreement	**States Involved**	**Primary Goals**
Informal meetings	China, Russia, and the US	Prevent escalation
Budapest Convention	62 states ratified; 4 signed, not ratified	Common criminal policy
United Nations Group of Government Experts (UN GGE)	Rotating membership based on region, including Security Council countries	Ensuring digital and information security
Shanghai Cooperation Organization (SCO)	China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India, and Pakistan; Afghanistan, Belarus, Iran, Mongolia; Azerbaijan, Armenia, Cambodia, Nepal, Turkey, and Sri Lanka	Primarily focused on its member nations' security related concerns
Internet Governance Forum (IGF)	Over 100 participating countries, with multi-stakeholder representation	Promote multi-stakeholder dialogue to discuss IG issues
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)	Austria, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, Turkey, the UK and the US	Coordinates education and training on cyberdefense
Tallinn Manual	Academic, non-binding; no official members	Increase understanding of international law in cyberspace
Additional noteworthy agreements		
International Agreement	**Member States Involved**	**Primary Goals**
Wassenaar Arrangement	42 participating states	Exchange information
International Multilateral Partnership Against Cyber Threats	152 states signed; first UN-backed cybersecurity alliance	PPPs against cyberthreats

Background

As Information and Communications Technology (ICT) continues to increase global connectivity, the proliferation of cyberattacks become more advanced and frequent. In fact, threat assessments predict that the next international crisis could be the result of a cyberattack weaponizing ICTs to alter or

destroy critical infrastructure (Council on Foreign Relations, 2018). An increase in interconnectivity with technologies such as Internet of Things (IoT), persistent threats of Distributed Denial of Service (DDoS) attacks, ransomware, and other methods of attacking threaten industry, government, and society.

Emerging cyberthreats, combined with a plethora of other security issues – including cybercrime, cyberespionage, data privacy infringements, and many others – necessitates cooperation among nations to mitigate risk under an international standard. International agreements can effectively curtail the efficiency of emerging cyberthreats that otherwise could have lasting, damaging societal and economic implications. Although currently there are a multitude of organizations, councils, informal meetings, and conventions seeking to unite the globe under a single standard, there is a lack of global unity as many countries reject drafted policies. Regardless, there is an effort to create a unified code of conduct, and recent legislation efforts seek to create an implementable global strategy.

International Law of Armed Conflict in the Context of Cyberspace

An overview of pre-existing international agreements of cyberspace shows that the idea that international law applies to cyberspace is generally accepted by the international community. Where the agreement becomes more difficult is in deciding the practical application of traditional rules of war and tailoring law of armed conflict to cyberattacks and cybersecurity. A basic understanding of customary international law of armed conflict is important to understanding the sources of contention.

Cyberoperations, the use of cybercapabilities to achieve objectives in or using cyberspace, can be used to cause physical damage, injury, loss of life, or harm to infrastructure (Schmitt, 2041). This leads to questions of how to respond to such acts and whether they meet the threshold of armed force, which then leads to traditional principles of war and armed conflict. While states continue to disagree about pre-existing international law of armed conflict's application to cyberspace, it is important to understand basic notions of law of armed conflict and their implications for cyberspace.

The threshold for cyberoperations to qualify as cyberwar remains high by global consensus (Ducheine, 2015). However, the question stands of whether cyberoperations that fall short of cyberwarfare but nonetheless create substantial harm are still considered use of armed force. It would seem that cyberoperations causing physical harm violate Article 2(4) of the UN Charter, which prohibits all UN members from threatening or using force against the "territorial integrity or political independence of any state" (Roscini, 2015). A number of states have previously agreed that not only the UN Charter but also other pre-existing rules on the use of armed force apply to cyberspace (Roscini, 2015). These rules do apply to armed force, and there has been no definitive answer as to what level of

operations qualifies as “armed” or not, especially as it becomes increasingly possible to cause significant harm to state’s and their infrastructures using non-destructive methods (Roscini, 2015).

This question of degree becomes even more significant in the context of the existing law of armed conflict, specifically the principles of *jus ad bellum* and *jus in bello*. *Jus ad bellum* refers to the customary rules and criteria that need to be met or consulted before entering into armed conflict or declaring war. *Jus in bello* refers to the customary rules for conducting warfare to limit unnecessary and disproportionate suffering. The unique characteristics of cyberattacks and even cyberwarfare make it difficult to apply the balancing tests of *jus ad bellum*. The disparate nature of cyberattacks and focus on secondary consequences—manipulating networks and systems rather than causing immediate mass destruction, for example—make it difficult to identify a single moment of armed force that in itself justifies the choice of going to war (Bannelier-Christakis, 2015). Although traditionally the rules of *jus in bello* apply only after state actors have publicly declared war, it may be important to consider the complex nature of *jus in bello* principles in the context of cyberwarfare. The serious distinction between civilians and combatants and their respective rights during war, for example, does not have a clear translation to cyberspace. The principle of distinction, which determines how military options are directed based on the necessary protection of civilians and non-combatants, was formulated in times of war and military operations. But as cyberspace becomes increasingly interconnected across states and actors, the distinctions between civilians, the military and who qualifies as combatants continues to blur, complicating the principles and making enforcement challenging (Bannelier-Christakis, 2015).

Existing Agreements

The current state of international cybersecurity agreements and norms is disparate across regions and increasingly divided according to ideologies on internet governance. As a result, there is a lack of binding language or mechanisms for accountability in terms of instances of cyberattacks and cyberwar. Looking at existing non-binding agreements on cybersecurity and collaborations between stakeholders provides insight into re-affirmed principles across regions and organizations, which serves to highlight not only areas of contention but potential areas of agreement in the future.

Informal Meetings

In the case of US, China, and Russia, the international dialogue is often one of conflict. Russia’s malware commonly targets US power grids; Chinese attackers target personal data and intellectual property of US corporations; and the US has, although only allegedly, been involved in offensive cyberattacks against both (Lake, 2019). Despite their differences, these three countries continue to have bilateral meetings that serve to prevent a spiral of escalation in cyberspace and have stability as the

primary concern. These meetings are beneficial in that they increase the level of understanding between the nations and provide one another with a general idea of the capabilities of their counterparts (Lake, 2019). Although informal diplomacy of this type is not a classic methodology way to curb cyberwarfare, it is a stepping stone.

In terms of bilateral relations, the US has engaged with China and Russia individually to address issues pertaining to cybersecurity. In August 2018, the Kremlin proposed a cooperative agreement with the US to prevent cyberattacks on critical infrastructure (Grisby, 2018). Although nothing came to fruition, this was the third time in two years that Russia has requested alliance and cooperation on cyber issues. Grisby notes that this may be for three reasons: skepticism of sincerity in Russia's offerings; Russia and the US fundamentally disagreeing with one another on issues and the nature of cyberconflict; and, that under the Trump Administration, an agreement would warrant an incredulous response in light of the 2016 election interference (Grisby, 2018). In contrast to the US and Russia's inability to reach a cooperation agreement, in 2015, former President Barack Obama signed an agreement with China's President, Xi Jinping, that outlined cyberrelations between the two countries (Rollins, 2015). The two countries agreed to provide timely responses to malicious activities, refrain from theft of intellectual property, and pursue appropriate norms of behavior in cyberspace. Although the quantity of attacks has dropped dramatically since the agreement, a US intelligence official stated that regardless, China has been violating their agreement with the US (Bing, 2018).

Budapest Convention

The Budapest Convention, formally known as the Convention on Cybercrime of the Council of Europe, is the first and only multilaterally binding international instrument for cybercrime regulation (Council of Europe, 2018). As of January 2019, 62 states have ratified the convention, and another four have signed but not ratified it (Council of Europe, 2019). The convention's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international cooperation (Council of Europe, 2018b).

The Budapest Convention is an important asset in harmonizing cybercrime laws to combat cybercrime on a global scale, and as noted by Clough, harmonization is pivotal for two reasons. The first is to reduce the possibility of "safe-havens," or locations where otherwise illegal conduct is not criminalized. The second is for effective and efficient communication between law enforcement agencies (Clough, 2014). However, there are difficulties in achieving this harmonization.

Although the Budapest Convention is an ongoing attempt at creating global cybercrime regulations, it is extremely difficult to achieve full international cooperation. Russia, for example,

released their own proposal for a new "United Nations Convention on Cooperation in Combating Information Crimes" in 2017, stating that the Budapest Convention was a threat to the sovereignty of the country (Ignatius, 2017). Russia is not alone in their sentiments. Other countries, such as China, argue that the treaty is inherently inapplicable to non-European countries since they did not have a hand in its creation, despite the fact that non-European countries are party to the convention (Grisby, 2014).

The Budapest Convention does not directly interact with cyberwar norms, and primarily focuses on international unity of cybercrime policies. While this does provide a basis for governing cyberconflict, the current framework only goes so far to bring existing international law to bear on cyberconflict (Eilstrup-Sangiovanni, 2018). This draws attention to the lack of existing international cooperation around cyberwar and calls for a cyberwar convention to govern conflict between nation-states.

United Nations Group of Government Experts (UN GGE)

The UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security is a UN working group on digital and information security (Digital Watch Observatory, n.d.). First established in 1998, it convenes every few years to conduct closed door sessions that result in official reports that carry significance in the field of global cybersecurity (Digital Watch Observatory, n.d.). From 2004 to 2013, the UN GGEs contained 15 members; each UN GGE included the UN Security Council countries with the remaining seats allocated by the UN Secretary-General with a focus on equal regional representation (UNIDIR, 2016). The 2014-15 UN GGE was expanded to 20 members, and the 2016-17 and 2019-21 UN GGEs were both set at 15 members (UNODA, 2019).

A notable development from the 2013 UN GGE report was the application of customary international law, particularly state sovereignty and multilateral accords such as the UN Charter, to cyberspace (UN GGE, 2013). The 2015 UN GGE report built on the 2013 report by stating that a state “should not conduct or knowingly support [Information Communications Technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure” (Maurer, 2016). The report further stated that state must not use proxies or non-state actors to commit wrongful acts using Information Communications Technology and should attempt to keep their own territory and infrastructure from being used by non-state actors to commit such acts (Maurer, 2016).

Following these groundbreaking developments, the 2017 GGE failed to reach a consensus on a final report (UN GGE, 2017). A statement from the Cuban UN GGE Representative at the conclusion of the 2017 GGE attributed this breakdown of discussion to the serious concerns about the intent of

powerful state actors to use cyberspace as a "theater of military operations" against the interests of weaker states (Rodríguez, 2017). In contrast, the US Representative to the 2017 GGE blamed the lack of consensus on an unwillingness from the part of states to apply international law to cyberspace. Without this application, states would be free to use cyberspace for their political ends without limits (Markoff, 2017). The US Representative advocated for using existing international law framework to hold states accountable for their actions in cyberspace (Markoff, 2017). With the sixth UN GGE set to start meeting in 2019, the possibility of future consensus by the working group remains uncertain.

Shanghai Cooperation Organization (SCO)

The SCO started as a collaboration between China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan (Albert, 2018). India and Pakistan recently became the newest full members (Usmanov, 2018). In 2011 and 2015, Shanghai Cooperation Organization members proposed the International Code of Conduct on Information Security, a proposed annex to the discussion of international cybernorms, to the UN (Grigsby, 2015). The Code reaffirmed the rights of states to protect their own cyberspace and cyberinfrastructure (Letter to the UNGA, 2011). However, the US and other Western countries dismissed the code as an attempt to institutionalize greater state control over cyberspace (Grigsby, 2015).

Language from the International Code of Conduct was included in a UN resolution proposed by Russia in late 2018 (Grigsby, 2018). In response, the US proposed a competing resolution in partnership with EU countries, Canada, Australia, and others absent of any language from the International Code of Conduct that called for the UN GGE to international law's application to cyberspace (Grigsby, 2018).

In addition to member states, the SCO includes the observer states of Afghanistan, Belarus, Iran, and Mongolia; and the dialogue partners of Azerbaijan, Armenia, Cambodia, Nepal, Turkey and Sri Lanka. After applying for full membership in 2018, Iran has been actively lobbying to fully join the organization; furthermore, the presidents of both Russia and China have both expressed their support (Scita, 2018). The inclusion of Iran could serve as a catalyst for other Middle Eastern countries, particularly those affiliated with Iran through the Gulf Cooperation Council such as Saudi Arabia, Qatar, Bahrain, and the United Arab Emirates, to also request SCO membership (Fulton, 2018). Such an expansion, coupled with continued collaboration on cybersecurity norms, could make the SCO a significant counterpart to the Western-oriented multi-stakeholder approach to internet governance.

The conflicting resolutions and the statements from Cuba and the US following the 2017 UN GGE reflect underlying disagreements among actors about the relationship between international law and cyberspace. By the end of 2018, the UN established the sixth UN GGE to start in 2019 and report to the UN General Assembly in 2021 (Digital Watch Observatory, n.d.). Concurrently, the UN established

two additional working groups aimed at discussing norms and principles for state behavior in cyberspace (Digital Watch Observatory, n.d.). The consequences of these different UN-sponsored groups studying cybersecurity norms and principles will be interesting to watch moving forward.

Internet Governance Forum (IGF)

The IGF is a policy dialogue forum that was established in 2006 by the UN Secretary-General as a result of momentum from breakthrough discussions on Internet governance within various organizations such as the International Telecommunication Union (Touré, 2011). It was created to build on this momentum and promote dialogue between civil society, industry, the technical community, and other stakeholders to discuss issues of internet governance (Electronic Frontier Foundation, n.d.). The IGF meets annually in different countries and serves to facilitate dialogue across sectors, countries, and government, though it cannot make policy itself (Free Software Foundation Europe, n.d.).

The November 2018 IGF held in Paris, France was opened by remarks from French President Emmanuel Macron, who called on the international community to take on greater responsibility of internet regulation and cybersecurity norms (Ermert, 2018). The 2018 forum resulted in the Paris Call for Trust and Security in Cyberspace, a declaration in favor of common principles of Internet governance. Supporters of the Paris Call include 64 states, 328 private sector entities, and 129 international and civil society organizations (Ministry for Europe and Foreign Affairs, 2018). The IGF and the affiliated Paris Call represents a forum that embraces and promotes the multi-stakeholder approach, with participation across governments, private sector entities, and civil society organizations.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

The CCDCOE is an organization promoting understanding of the legal, technological, and research aspects of cyberconflict through conferences, cyberdefense exercises, and reports (CCDCOE). The Centre coordinates research, education, and training on cyberdefense and cyberwar for NATO-affiliated groups and countries (NATO, 2008). First established in May 2008 by an initiative from Estonia in partnership with Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain, the Centre has since grown to include 21-member nations inside and outside the NATO Alliance (CCDCOE). The core mission of the CCDCOE is to foster cooperation across member states, develop innovative approaches to international norms, promote regional capacity to protect against cyberattacks and related threats (Plantera, 2018). One of its flagship projects is the Tallinn Manual, a comprehensive and interdisciplinary analysis of how technology and law are implicated in cyberspace (Plantera, 2018). Based on the most recent reports to the UN Secretary-General on developments in individual member state regarding international cybersecurity, capacity-building and confidence-building is among one of the top priorities

for protecting against future cyberattacks and promoting international cooperation in cybersecurity (United Nations General Assembly, 2017). The CCDCOE could serve as a model for providing states with important education and training on building capacity and improving cybersecurity across borders.

Tallinn Manual

The Tallinn Manuals (2013/2017) are one of the most notable accomplishments of the CCDCOE and serve as a starting point for understanding existing international law in the context of cyberspace. Tallinn Manual 2.0 applies the traditional principle of sovereignty to cyberspace, establishing that that states must not violate the sovereignty or intervene in the internal and external affairs of another state through cyberoperations (Tallinn Manual 2.0, 2017). When operations conducted from the territory or infrastructure of a state have substantial negative effects on another state, the Manual holds that the former must exercise due diligence in stopping the harm (Tallinn Manual 2.0, 2017). Notably, the UN GGE only held that states "should" exercise due diligence. Rule 15 in Tallinn Manual 2.0 attributes actions of State organs to the state but distinguishes non-state actors as being outside the control of the State and therefore un-attributable to the state (Jensen, 2017). However, if a state subsequently adopts the actions of non-state actors as their own, then the actions are attributable to it (Jensen, 2017). The Manual writers noted that the high threshold of attribution will likely come under pressure as more and more states become victims of un-attributable cyberactivities (Jensen, 2017).

Areas of International Contention

An analysis of existing international agreements depicts a less than unified globe in the realm of cybersecurity. Although unifying agreements exist and attempt to function as a cooperative platform that assists in the unification of cybersecurity law, defense, media literacy, and partnerships – it remains difficult to leverage complete international cooperation. Areas of international contention that contributing to the lack of cohesion are infringements of national sovereignty, economic relations, conflicting ideologies of Internet governance, and lack of involvement in the legislation process.

One of the primary areas of concern that limits international cooperation for countries such as Russia and China is national sovereignty. In the Budapest Convention and many other international agreements, Russia and China refrained from signing as they saw it as an infringement on their national sovereignty. Moreover, based on recent legislation proposals, Russia aims to ban the publication of dissenting materials mentioning the Russian society, state, constitution, and law enforcement agencies (Sherman, 2018). Clearly, Russia has differing opinions on Internet regulations than other parts of the world, which may, in effect, be an underlying factor in their reluctance to join any international agreement. China offers similar contentions; however, China's opposition is mainly due to a

disinclination to engage in information and intelligence sharing (Hakmeh, 2017). Regardless, Russia and China continue to avoid international agreements to protect their national sovereignty.

Economic relations are another area that affects a country's international orientation and may prevent a country from engaging in international agreements if the economic alliance influences their orientation to international governance. An example of this would be South Africa. South Africa has strong multilateral economic relations through the Brazil, Russia, India, China and South Africa (BRICS) coalition. Of these, South Africa predominantly focuses its attention on Russia and China for economic support in ensuring stability and development. As a result, South Africa's international orientation leans towards that of Russia and China, which impacts the way it engages on certain topics. In the case of cybersecurity, South Africa commonly votes with Russia and China; this alludes to the fact that economic relations may impact a country's willingness to engage in international cybersecurity practices. However, countries like Saudi Arabia, India, and Brazil illustrate a different perspective. All want a say in international internet governance and are often frustrated with the US defining terms during legislation processes; a slightly different, yet equally important, reason for internet governance orientation.

The conflicting ideologies across major state actors makes coordinating the drafting of cybersecurity legislation and achieving consensus difficult. The unpredictability of cyberspace and increasing number of offensive cyberattacks make it difficult for major actors to agree to binding norms that would limit their ability to protect against such attacks or even use offensive action to strike back. While the US and Western-oriented countries prefer a multi-stakeholder approach that incorporates private and non-state actors in a cybersecurity framework, actors such as Russia, China, and India disagree with this approach and prefer to (Nocetti, 2015). Moreover, whether or not states are included in the drafting of cybersecurity agreements can be dispositive of whether or not those countries are willing to sign and ratify the agreements. India, like China and Brazil, initially declined to sign the Budapest Convention because it was not involved in writing the legislation (Javaid, 2018).

In achieving international agreements, states such as North Korea represent a complicated step towards that broad agreement. North Korea as a cyberactor is characterized by continued low-intensity operations and a strong sense of self-reliance, which disincentivizes cooperation with other states (Jun, et al., 2015; Armstrong, 2013). The willingness of North Korea to operate independently as an outlier to the broader international community in opposition to the US and other Western countries represents a potential threat to international agreement supported or influenced by US interests.

It remains difficult to reach a global consensus on how to engage in international cooperation, and many countries have differing contentions with the presently existing efforts to do so.

Major Offensive Actor: China

By Zhiqin Gao

Table 2: Summary Findings, China

Major Attacks	
Attributed Threat Actor	**Actor Intent and Actions**
U.S. Government: National Security Agency (NSA)	Espionage
Anti-Communist Hacker (反共黑客, *fangongheike*)	Political motives
Barbaros-DZ (individual Algerian hacker)	Defaced Chinese government websites
Flame/Flamer/ sKyWIper (unattributed APT)	Infected systems through USB or phishing emails
Iranian Cyber Army	Defaced China's popular search engine, Baidu
HangOver (APT-C-09, possibly India)	Information gain
North Korea	WannaCry - financial gain
Prolific Threat Actors	
US hacking for acquiring sensitive information and engaging in espionage	
Defensive Landscape	
Policies	**Protections Provided**
National Security Law	Prioritize security and control of Chinese cyberspace
Counter-Terrorism Law	Empower public security and military organs to employ technological investigative measures
Cybersecurity Law	Provide measures and guidelines for cybersecurity
Government Institutions	**Notable Publications**
Central Cyberspace Affairs Commission	Documents on cyberspace regulations
Ministry of Public Security	Rules on Critical Information Infrastructure Security
Central Commission/National Bureau of State Secrets	Administrative Measures (for Information Security)
State Encryption Administration	Draft of Cryptography Law
Ministry of Industry and Information Technology	Weekly/quarterly reports on China's cybersecurity
CNCERT	Consistently reports on China's cybersecurity
Industry Collaboration	**Products**
Enterprises: Huawei, ZTE, Datang Telecom Group, China Mobile, China Telecom, etc.	Research and Development, design, Chinese telecommunication products for military
Tsinghua University, Shanghai Jiaotong University	Research and Development, cyberwarfare training
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Sino-Russia Cybersecurity Agreement	Establish cooperation in international information security through joint solutions and dialogues
China-U.S. Cyber Agreement	Establish cooperation on combating cybercrimes and mitigating malicious cyberactivities
China-Australia Cyber Agreement	Bilateral legal framework against cybertheft
China-Laos Memorandum of Understanding	Bilateral legal framework on cyberspace cooperation
BRICS (Brazil, Russia, India, China and South Africa)	Cooperation framework on the digital economy and distributed ledger technology (DLT)

Introduction

China's orientation towards creating international cybersecurity norms can be assessed by reviewing its robust profile of major adversaries and cyberattacks, sovereignty-based cybersecurity policy landscape, and behavior at international meetings. China's strategically defensive cybersecurity policies could be particularly helpful in shaping international cybersecurity norms. In addition to its political background, the cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspectives seen within China implies that trust-building processes and power-sharing efforts will be essential to have China's cooperation in creating future international cybersecurity norms. Table 2 summarizes the findings of this case study.

Background

China's exploitable sociopolitical vulnerabilities are mainly structural. On one hand, China's party-state system faces challenges from hacktivists and nation-state actors who advocate against internet borders and the ruling of the Chinese Communist Party (CCP). On the other hand, the Chinese internet has been built with network security technologies from foreign countries, which makes its network security vulnerable from intrusions by foreign actors.

Sociopolitical Vulnerabilities

China's approach to cybersecurity carries the historical tradition of strategic conservatism in national defense. However, China's aggrandized national strength and assertive international behaviors in the recent past have caught the attentions of malicious actors who seek to exploit China's sociopolitical vulnerabilities.

At the state level, China lacks a clear legal framework that can be properly implemented in cyberspace, while different national bureaus and departments issue their own policies for cybersecurity that are sometimes contradictory. Rules and regulations of the internet are poorly enforced and applicable cyberlaws at different levels of administration are still underdeveloped (Lindsay, et al., 2015). At the societal level, the lack of education on cybersecurity and insufficient protection on individual privacy makes the Chinese public vulnerable from cybercrimes and cyberbullying. At the international front, the CCP's ruling faces challenges from hacktivists and nation-state actors who seek to push liberal democratic values internationally. Fears of "color revolution" or regime change by foreign and domestic actors make it hard for China to accept an internet without filters, which limits the room for China to cooperate on free internet-based international internet governance initiatives (People's Daily, 2019).

Level of Connectivity

China (Mainland)'s Information and Communication Technology (ICT) index is valued at 5.60, ranking 80th globally (ITU, 2017). In China, 55% of households own a computer, 59.6% of households

have internet access, and 54.3% of individuals use the internet (ITU, 2017). The growing integration of the internet into Chinese households suggests increasing vulnerabilities from cyberespionage and cybercrimes, although Chinese cyberspace regulation has increased along with the number of users

Major Threat Actors

Although attributing actors to cyberattacks is challenging, it is possible. Major actors who have conducted cyberattacks against China can be categorized into three groups: nation-state actors, hacktivists, and loose Advanced Persistent Threats (APTs).

The most prominent nation-state actor is the US government. For example, the revelation of Edward Snowden shows that the National Security Agency (NSA) has been gathering information through Huawei routers and switches and monitoring Huawei top executives' communications for years (Sanger, 2014). According to China's 360 Helios Team report in 2018, the Poison Ivy [hacking] Group has engaged in cyberespionage for eleven years against critical Chinese agencies with a strong interest in China-US relations, cross-Strait relations, and maritime issues (360 Helios Team, 2018). Although the report does not explicitly attribute attacks, a major IP address involved was traced to the US.

According to Chinese official sources, China's Ministry of National Defense was attacked 144,000 times per month in 2012 and 62.9% of those attacks originated from US IP addresses (Zhao, 2013). The National Computer Network Emergency Response Technical Team of China (CNCERT) reported that US-based cyberattacks constituted 83.2% of 2013's phishing activities targeting Chinese internet servers (Tang, 2013). As China-US relations become increasingly confrontational, suspicions of the other's intentions will intensify as the number of US-based cyberattacks against China continues to grow.

In addition, hacktivists and loose APTs on the internet challenge the control and stability of the Chinese state. Hacktivist groups such as Anonymous and the Anti-Communist Hacker (反共黑客, *fangongheike*) deface Chinese government and general websites as a way to protest the Chinese government's censorship and the CCP's ruling (Protalinski, 2012). Also, actions of probable APTs, such as Flame or WannaCry, have done serious damage (Xinhua, 2017).

Pattern of Attacks

Cyberattacks against China generally aim to acquire data or intelligence, advocate for opposing political ideologies, and seek financial gain. Most attacks on China's infrastructure concentrate on military, technology, and education industries and networks. Contentions between nation-state rivals pose the most serious national security threats because state-sponsored cyberattacks are often the most sophisticated ones. Moreover, as power diffuses to individuals in the international system with the empowerment of the internet, another pattern of attacks is for sending political messages.

In the case of China's cybersecurity situation, the US is identified as a frequent attacker for data and intelligence gathering. The Snowden leaks revealed that the NSA has hacked into the system of Huawei, a Chinese nationally-championed telecommunication company, for surveillance and acquisition of sensitive information (Sanger, 2014). While the US was attributed to this attack, additional unidentified actors also attack for intelligence. For instance, Symantec reported in 2016 that cyberespionage group Strider specifically targeted a Chinese airline company for data and information theft, though the intentions and attribution are unclear (Symantec, 2016).

Hacktivist groups such as Anonymous, who advocate against censorship, for example, often attack Chinese government websites and reveal administrators' information online to challenge the regime's dominance. The Iranian Cyber Army, an organized hacking group, defaced Baidu, China's largest search engine, in 2010 (BBC, 2010). Individual hackers also target China, such as the Algerian hacker Barbaros-DZ (Kovacs, 2013).

Financial gain is a major pattern of attacks against China. Most notably, the 2017 WannaCry incident is a proper example of ransomware attack that greatly disrupted Chinese people's, especially students', everyday lives, given that the WannaCry attack happened during China's national college entrance examination period. Other APT attacks such as Flame and Hangover caused serious economic and psychological damage to Chinese civilian network in cyberspace, especially to the business communities and research/educational institutions (51CTO, 2012; SecPulse, 2016).

National Cybersecurity Strategy

China has a strategically defensive, operationally offensive cybersecurity doctrine. To counter threats and maintain control, China's cybersecurity strategy emphasizes the necessity of safeguarding internet sovereignty, civil-military cooperation on preparing cyberwarfare against major rivals and international cooperation on combating cybercrimes.

Offensive Cybersecurity Strategy

Based on the analyses by foreign sources, China has conducted extensive cyberespionage, although the Chinese government denies involvement in any of them. Assuming all the acquired information on China's cyberattacks is credible, this report concludes that China mainly attacks for maintaining the ruling of the CCP, supporting national interests, and safeguarding economic development.

To support China's Anti-Access/Area-Denial (A2/D2) strategy for air-sea battle in the Western Pacific, China's operationally offensive cybersecurity doctrine is rooted in the belief that information superiority stems solely from conducting offensive information operations (Zhang, 2006). While China

operates a passive defense mode over civilian use of cyberspace, the military operates in an active defense posture because first use capabilities and commitments in information warfare are considered crucial to counter rivals with stronger capabilities such as the United States. Chinese security analysts characterize the attack on command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR) as decisive for successful military campaign in modern warfare (Guo, 2008). However, there is a lack of Chinese cybersecurity literature on the complexity of kinetic warfare in practice and the consequences and misperceptions of cyberstrikes.

Offensive operations that are attributed to China often concentrate on intelligence gathering, corporate espionage, and signaling deterrence to political dissidents. Based on publicly available information, Chinese cyberespionage can be traced as far back as the 2003 "Titan Rain" attack that targeted US defense organizations and national scientific labs (Thornburgh, 2005). Other noteworthy attacks targeting official agencies include "Byzantine Haydes" (2002) and Shady RAT (2006), both of which severely compromised many US government agencies' networks and were identified by the US as APT intrusions from China (Glanz, 2010; Alperovitch, 2011).

Government agencies are not the sole targets of cyberattacks, as corporate espionage is also common. Aurora (2009) and F-35 Joint Strike Fighter (2007) are two well-known examples. The 2009 Aurora attack on Google prompted Google's exit from Mainland China (Cha, 2010). The F-35 Joint Strike Fighter attack, on the other hand, acquired data of a $300 billion high-profile target through networks of Pentagon contractors: Northrop Grumman, BAE and Lockheed Martin (Gorman, et.al., 2009). Besides intelligence gathering and corporate espionage, Chinese cyberattacks also target dissidents and human rights activists that challenge the CCP's ruling. For instance, in 2007, Ghost Net attacked Dalai Lama and government agencies and firms in 103 countries (Glanz, 2010). In 2009, Elderwood (Sneaky Panda), later being identified as a sophisticated Beijing-based APT group, attacked several human rights NGOs (Symantec, 2012). All three types of Chinese offensive operations in cyberspace serve the purpose of maintaining CCP's dominance, supporting national interests, and securing national economic development.

China's national cyberdefensive posture is based on the principle of sovereignty or territorial defense. Strategies of China's state-sponsored offensive operations come primarily from the People's Liberation Army (PLA), or the Chinese military. In particular, China's operations are mostly managed by the Third Department of the PLA General Staff Department (总参三部, 3/PLA) and the Fourth Department of the PLA General Staff Department (总参四部, 4/PLA). The 3/PLA exploits vulnerabilities

globally and defend the classified network domestically, while the 4/PLA oversees electronic countermeasures (ECM) and radar-related operations.

At the operational level, the 3/PLA has twelve bureaus, or units, each with distinct or overlapped missions. The First Bureau's mission may be to decrypt, encrypt, and focus on information security, and is likely to cooperate with relevant organizations in Sichuan (Stokes, et.al., 2011). With most offices located in Shanghai, the Second Bureau's mission may have a regional focus that specifically targets the US and Canada with an emphasis on strategic intelligence (Stokes, et.al., 2011). They have been identified as APT 1, or Comment Crew, which has targeted 141 English-speaking firms in 15 countries (Mandiant, 2004). The Third Bureau, with bases established across the country, may collect and detect radio communications, border control networks, and emission security (Stokes, et.al., 2011). The Fourth Bureau, located in Qingdao, is suspected to have a regional focus on Japan and Korea (Stokes, et.al., 2011). The Fifth Bureau may have a regional focus on Russia with its bases across China-Russia borders from the Northeast end to the Northwest front (Stokes, et.al., 2011).

The Sixth Bureau is suspected to have a regional focus on Taiwan and South Asia, given its offices located across China's east coast (Stokes, et.al., 2011). The Seventh Bureau's mission is more diverse, as evidence suggests there are specialists in engineering, foreign languages, and international law (Wanfang Data, 2016). The Eighth Bureau, given its members' language proficiencies, may have a regional focus on Europe, the Middle East, Africa and Latin America (Stokes, et.al., 2011). The Ninth Bureau, located near the Summer Palace in Beijing, may function as analyst for strategic intelligence and database management (Lindsay, et.al., 2015). The Tenth Bureau, as China-US diplomatic history suggests, may serve as a missile tracking or testing functions unit, with a regional focus on Central Asia and Russia (Tao, 2004). The Eleventh Bureau, with Russian linguists as members and established presence in Heilongjiang and Xinjiang, may have a regional focus on Russia. The Twelfth Bureau may serve to intercept and collect satellites communications (Stokes, et.al., 2011).

Policy Landscape

In April 2014, Chinese President Xi Jinping formally claimed at the first Central Cyberspace Affairs Leading Group meeting that "there is no national security without cybersecurity" (Xinhua, 2014). Following the top leadership's emphasis on cybersecurity, China has issued three strategy documents and introduced three legislations on regulating and cooperating in cyberspace since 2015 - China's Military Strategy, Cyberspace Security Strategy, International Strategy of Cooperation on Cyberspace, National Security Law, Counter-Terrorism Law, and Cybersecurity Law. Common principles developed within the strategy documents stress the significance of safeguarding internet sovereignty and security,

peaceful use of cyberspace, and fairness in internet governance and informationization (信息化) as an evolution of modern warfare.

China's cybersecurity policies demonstrated the "strategically defensive, operationally offensive" characteristic of China's overall cybersecurity doctrine. Although China's cybersecurity policies favor an international environment that limits cybercrimes so that the regime can be more secure, China's growing economy still depends largely, though now relatively less, on foreign core internet security technologies. While Chinese President Xi Jinping has been pushing for independent innovation in core industries since he came to power in 2012, it takes time for key heavy industries and telecommunication companies to outrun the path of innovation of developed economies like the US. Therefore, China may also favor the current cybersecurity environment in the sense that China can take advantage of difficult attribution and keep performing low-cost intelligence gathering and technology acquisition through cyberspace.

Tech Industry Collaboration

At the front of active military defense, China has developed robust civil-military cooperation among government, military, commerce, and education agencies. State-Owned Enterprises (SOEs) like China Mobile, for instance, have established information warfare militia units in several local branches to help maintain national network and communication security. Similar to corporate militias, military-related research institutes on information security and university-based information warfare militias units are established in several Chinese colleges and universities such as Tianjin Polytechnic University, Hainan University and South China Normal University to train students in technical skills and national security (Lindsay, et.al., 2015).

At the civilian level, China's Cyberspace Security Strategy encourages civil society's contribution to cyberspace governance. As an integral part of the Chinese economy, digital economy is emphasized in China's International Strategy of Cooperation of Cyberspace. In particular, the Chinese government stresses its support for internet-based entrepreneurs and the digitalization of industry, agriculture, and service sectors. China advocates for a stronger role of online business cooperation in both the formulating of cyberspace trade rules and the sharing of internet technology.

Education

China's cybersecurity strategies emphasize social education as a critical part of managing and innovating online social organizations, as well as protecting citizens' lawful rights and interests in cyberspace. In recent years, China began raising social awareness and public engagement on cybersecurity through propaganda and public education. In coordination with local police,

administrations at all levels announced a “Cybersecurity Education Week” that primarily focuses on educating young people and the elder on basic cybersecurity knowledge and measures to avoid phishing and cybercrimes (Liu, 2018). As internet users increase in China, the Snowden revelation, the WannaCry incident, and publicity of cybercrimes gradually have raised the societal awareness to take measures to protect privacy and security in cyberspace.

International Internet Governance

China has moderate involvement in international internet governance efforts because it prefers UN initiatives and regional agreements where the Chinese government can have a significant role to play. In recent years, China has actively participated in bilateral or regional cooperation in cyberspace with its neighbors and major powers as cybersecurity increasingly becomes a global concern.

Country Orientation

China emphasizes a multilateral approach through the UN for international cooperation in cyberspace. Recently, China has been pushing for the “Digital Silk Road,” as part of the nation’s Belt and Road Initiative to incorporate developing nations and several developed economies in Africa and the Eurasia landmass through geo-economic tools. The goal is for China to lead multilateral cooperation in international internet governance that combats cybercrimes and terrorism and accommodates China’s internet sovereignty concerns (Yang, 2016). The growing strategic rivalry between China and the US makes it challenging for China to cooperate in US-dominated international agreements.

Behavior at International Meetings

China favors international cooperation through the UN platform. Most notably, China is represented at the UN Group of Government Experts (GGE) on Development in the Field of Information and Telecommunications in the Context of International Security (UN, 2013). In addition, China hosted the International Cloud Security Conference in 2017 to promote international cooperation in information safety and the development and implementation of new information and telecommunications technologies (SCO, 2017). Meanwhile, China has been actively establishing bilateral and multilateral cooperation with other countries in cybersecurity since 2015 and is an active participant in regional cybersecurity cooperation. As long as there is no overstep on the principle of internet sovereignty in an international agreement, China generally welcomes opportunities for cooperation in cyberspace through either bilateral or multilateral approach.

US-China Alignment

The US and China signed a US-China Cyber Agreement in September 2015 and both countries agreed to cooperate with requests to investigate cybercrime, collect electronic evidence, and mitigate malicious cyberactivity emanating from their territories. Both countries agreed that neither will conduct

or knowingly support cyber-enabled theft of intellectual property. Additionally, both countries acknowledge the need to develop international cybersecurity norms and welcome UN GGE's report on information security. Through the bilateral cyber agreement, methods of communication, such as annual high-level dialogues and hotlines, are established to prevent crisis escalation in the cyberdomain between China and the United States (White House, 2015).

Shaping International Norms

China has a strategically defensive, operationally offensive cybersecurity doctrine. Its cybersecurity policies emphasize the need to cooperate internationally on the basis of internet sovereignty. However, China's military is actively prepared to fight information warfare as today's international cyberspace is still anarchical.

As the case study shows, China will advocate for sovereignty-based internet governance as international norms. China will agree with BRICS and SCO member states on the issue of cybersecurity norms internationally. The sociopolitical context of China and Chinese cybersecurity strategies reveal that internet sovereignty is absolute essential to the regime's understanding of international security.

As the world returns to great power rivalry, establishing common norms and vocabularies for international cybersecurity norms becomes more urgent than ever. To have China reaching a common ground on international norms with the US and other Western nations, multilateral cooperation on combating cybercrimes is a crucial first step for trust-building and power-sharing. Most importantly, international agreements without respect of internet sovereignty will be impossible for China to accept.

Major Offensive Actor: Iran

By Sara Koeck

Table 3: Summary Findings, Iran

Major Attacks	
Attributed Threat Actor	**Actor Intent/Damages**
US and Israel	Stuxnet attack on Iranian nuclear centrifuges in Natanz
Prolific Threat Actors	
US and Israeli forces	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Constitution of the Islamic Republic of Iran (1979)	Focus on the Islamic Revolution and Iranian sovereignty
Government Institutions	**Notable Publications**
Islamic Revolutionary Guard Corps (IRGC)	Ashiyande Digital Security Team work with Sun Army
Ministry for Information and Communications Tech	Annual budgetary report for ICT programs
Industry Collaboration	**Products**
China's Huawei company	Business in Iran in defiance of sanctions
Ashiyande Digital Security Team (IRGC)	Online forum for cyberattack and virus discussions
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Agreement on Cooperation – Iran	Investment in ICT, cybersecurity, and e-commerce
Joint Comprehensive Plan of Action (JCPOA)	Nuclear development deal to lessen sanctions on Iran

Introduction

Iran's orientation towards creating international cybersecurity norms can be assessed by reviewing its diverse profile of major adversaries and cyberattacks, limited cybersecurity policy landscape, and behavior at international meetings. Iran's attitudes toward international internet

governance could be particularly helpful in shaping international cybersecurity norms. In addition to its political background, the offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective seen within Iran implies that Iran will cooperate in creating future international cybersecurity norms. Table 3 summarizes the findings of this case study.

Background

Iran's background is filled with uncertainty amidst a fast increase in technology use and a quickly developing array of cybercapabilities.

Sociopolitical Vulnerabilities

The current supreme leader of Iran, Ayatollah Ali Khamenei, has considerable power in the state and in the country's religious ambitions for the Islamic Revolution. The internal tensions of Iran are a weakness that could potentially be targeted by other actors. Iran has negative opinions regarding the US, Saudi Arabia, and other actors that are anti-Iranian, which make its main goal in cybersecurity to remain sovereign in the face of outside actors (The Economist Intelligence Unit, 2019).

Level of Connectivity

Iran's Information and Communications Technology (ICT) index is 5.58, ranking 81st globally (ITU, 2017). In Iran, 70% of households have Internet access, and 60.4% of individuals use the Internet (ITU, 2017). Although these statistics indicate mediocre levels of connectivity, Iran's global rank is increasing in relation to information and communications technology. The ICT Ministry has dramatically increased its annual budgets to continue enhancing its connectivity (Keshavarz, 2017).

Major Threat Actors

Iran is predominantly attacked by the US and Israel. The only notable attacks against Iran were Flame and Stuxnet, which are both attributed to a combination of the US and Israel. The attacks were meant to damage the Iranian nuclear program and delay the nuclear advancements (Warrick, 2014).

Pattern of Attacks

The 2010 Stuxnet attack, believed to be a collaboration between the US and Israel, targeted Iranian nuclear centrifuges to setback Iran's nuclear program. The complex Stuxnet virus forced the centrifuges to spin out of control and require replacement (Tsagourias, 2015). It was preceded by a virus called "Flame" which collected intelligence before the attack (Nakashima, 2012). Stuxnet demonstrated that cyberattacks can do physical damage rather than just damage to software (Warrick, 2014). Stuxnet drove Iran to heavily invest in its cybercapabilities to be more readily prepared for both defensive and offensive maneuvers.

National Cybersecurity Strategy

The Islamic Republic of Iran has very impressive cybercapabilities, considering the age of these programs, which makes them a major actor in international cybersecurity. Iran has a wide range of actors and attacks within cybersecurity. Iran's policies regarding cybersecurity are very limited.

Offensive Cybersecurity Strategy

Iran has mostly attacked the US and Saudi Arabia, but other countries have also been attacked. Table 4 below outlines the major attacks, targets, and assumed motivations, as well as whether they are affiliated with the Iranian state directly or are independent actors within the country.

There are several state-affiliated and independent cyberactors within Iran. Since 2002, and even more so after Stuxnet, Iran has formed different groups under the Islamic Revolutionary Guard Corps (IRGC) to focus operations in cyberspace. Among these are the Ashiyande Digital Security Team and the Sun Army, which are the only actors known to be under the control of the IRGC and the Iranian state. Mostly, these two groups work to monitor social media within the country and abroad, and censor the information coming in and out (Keshavarz, 2017). Ashiyande also monitored an online forum, which gave individual hackers to show off their abilities while discussing different viruses (Fazzini, 2019). The forum was eventually shut down by Ashiyande in 2018. Other actors who conduct cyberattacks are not knowingly affiliated with the state and include larger groups or seemingly-individual hacktivists called "kittens" (Kirmeier, 2019). Among these is the Cutting Sword of Justice who in 2012 initiated a major cyberattack against the Aramco oil company in Saudi Arabia (Perlroth, 2012).

Iran's cyberattacks tend to be smaller in scale with a few exceptions of larger attacks. As a response to Stuxnet, the types of attacks have become more sophisticated. They range from website defacement attacks, to data hacking, DDoS attacks, and political disinformation campaigns (Stubbs & Bing, 2018). The main motivation for these seems to be the spread of political and Islamic opinions against the anti-Islamic and anti-Iran commentary of the United States and Saudi Arabia.

Table 4: Major Attacks and Targets

Actor	Attack	Target	State Affiliation	Assumed Motivation
Ashiyande	NASA – Website Defacement	USA	Yes, under IRGC	Anti-Americanism
The Sun Army	NASA – Website Defacement	USA	Yes, under IRGC	Anti-Americanism
Cutting Sword of Justice	Aramco – Shamoon	SAU	Not confirmed	Anti-Saudi Arabia
Izz ad-Din al-Qassam	Operation Ababil; DDoS	USA	Not confirmed	Retaliation for Stuxnet
Hamid Firoozi	Bowman Avenue Dam – hack on operations	USA	Not confirmed	Anti-Americanism
Other	Navy Marine Corps Intranet – disruption, no loss of data	USA	Not confirmed	Anti-Americanism
Other	Sands Casino, Las Vegas – daily logistics obstruction, data theft	USA	Not confirmed	Retaliation for Anti-Iran rhetoric

Policy Landscape

Regarding formal policies and strategies, Iran has very limited, publicly available information regarding the actual cybersecurity policies of the country. There is no official document outlining Iran's cybersecurity policies of cyberwarfare strategies (Shafqat & Masood, 2016). However, there was a 95% increase in budget for the Ministry of Information and Communications Technology for the 2014-2015 financial year (Keshavarz, 2017). The closest thing that can be analyzed for Iran's intentions is its constitution. The constitution of Iran (1979) outlines major themes for Iranian foreign policy, such as continuing the Islamic Revolution and staying independent from outside influences (Islamic Republic of Iran, 1989). This is to be analyzed when thinking of their cybersecurity actions, as it can explain motivation for past attacks against anti-Islamic and anti-Iranian actors. Apart from formal policy, Iran has a Computer Emergency Response Team (CERT), also known as MAHER, which has been in communication with other nations' CERTs regarding new viruses and past attacks (Higgins, 2012).

Considering the constitution, the presence of the Computer Emergency Response Team, and the importance of the Islamic Revolution, the driving force for Iran's cybersecurity seems to be more concerned with religious and political agendas rather than financial gains. Assuming nothing changes in the political landscape, it is unlikely that Iran will state formal cyberstrategies and policies to the international community in the near future, unless incentivized by economically beneficial deals.

Tech Industry Collaboration

The amount of ecommerce and tech companies within Iran has increased, but major US companies still refrain from operating within Iran due to economic sanctions that the US placed on Iran

(Reuters, 2017). China, however, has a clear presence within Iran's industry through the company Huawei and other smaller companies (Rapoza, 2019). Within Iran, many new start-ups are working to build apps that are similar to US apps unavailable to Iranians, as the percentage of Iranians who have smartphones continues to grow (Dorigo, 2016).

Education

In regard to education in technology and incident management training, Iran is ahead of many Western countries. A very high percentage of Iranians received a college degree from US or European universities before returning to their home country (Dorigo, 2016). More women are educated in a STEM field than any other country. Also, the percentage of the population that owns smartphones has increased dramatically in recently, which adds to the media literacy of the population (Merelli, 2018).

International Internet Governance

Looking at Iran's attitudes towards the US and other major players in international internet governance, it can be inferred that Iran is not opposed to international internet governance, as long as the US is not the most powerful actor within the system.

Country Orientation

Iran's orientation towards international internet governance has been changing from an isolated to a more open perspective. In previous years, Iran attempted to create a national intranet to remove itself from the World Wide Web and strengthen the government's control in cyberspace (Dehghan, 2012). In addition to the country's desire to censor and control the internet, its constitution emphasizes the need for independence from other countries and actors. However, current relations between Iran and countries like China suggest that Iran is not completely opposed to International Internet Governance, so long as the power within the organization is not solely with countries like the US that have a subpar relationship with Iran. Iran's main concern in this discussion is to ensure that it maintains sovereignty within an international system.

Behavior at International Meetings

Delegates from Iran have been present at the Internet Governance Forum (IGF) in the past few years. Starting in 2015, the attendance of Iranian delegates both onsite and online increased, on average, from one delegate to four. The increase may come from the higher budget for the Information and Communications Technology Ministry (ICT), as well as increased tensions between Iran and other countries (IGF, 2017). Specifically, at the 2017 Internet Governance Forum, a senior adviser to the Deputy Minister of ICT attended panels on the topics of Digital Activism and how they reshape the internet, challenges with digital identity management, as well as a panel about political disinformation through media.

From this information, the increased attendance of delegates at the IGF hints to Iran's willingness to listen to what other international players have to say or at the least, its desire to understand other nation's perspectives on cybersecurity and cyberwarfare. However, the country does not seem keen to adding its own perspectives to the discussions, or to build up relationships with other nations in regards to cybersecurity. The assumption is that Iran will continue to attempt staying independent from the international community.

US-Case Country Agreement

There are certain areas of potential agreement between Iran and US in terms of cybersecurity. Both Iran and the US did not sign the Paris Call, which implies that specifics in the document did not appeal to the two countries, and that future documents may do a better job of incentivizing both countries to sign the agreement (Uchill, 2018).

One of the biggest barriers between Iran and the US to potentially agree on cybersecurity is the ubiquitous tension between the two nations. Most of the tension comes from events in recent years such as Stuxnet, US sanctions on Iran, and the Iran Nuclear Deal, as well as the opposing political stances of the two nations that will potentially lead to an increase in cyberattacks in the future between the US and Iran (Perlroth, 2018). In terms of international cooperation, Iran is less likely to sign a deal in which the US is the most prominent power.

Shaping International Norms

Moving forward, it seems likely that Iran will be able to agree to certain international cybersecurity agreements, given very specific circumstances. Due to already existing tensions and previous cyberwarfare between the US and Iran, Iran is unlikely to agree to policy proposed by the US or in which the US holds a substantial amount of power. Iran is more likely to join an agreement that is either proposed by a more neutral country, or by countries such as China and Russia that value the sovereignty of nation-states as much as Iran does. Examining Iran, it is important to consider how relations with other countries and their policies must be acknowledged when attempting to create a functional and realistic international agreement for cybersecurity.

Major Offensive Actor: North Korea

By Nick Drainville

Table 5: Summary Findings, North Korea

Major Offensive Attacks	
Attributed Actor	**Actor Intent/Damages**
APT37	The Fourth of July Incident -- DDoS attacks
Lazarus	Sony Hack -- released and deleted data SWIFT Network Bank-- $81 million stolen WannaCry -- global ransomware attack
Prolific Offensive Actors	
Lazarus, APT 37, APT 38, Bureau 121	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Low-intensity attacks	Draws less attention to the DPRK
Disconnected internet access	Means it is less vulnerable to attack
Government Institutions	**Notable Publications**
The Reconnaissance General Bureau	N/A
General Staff Department	N/A
Industry Collaboration	**Products**
Unicom (China)	internet
TransTeleCom (Russia)	internet
International Orientation	
North Korea has not signed any multilateral or bilateral agreements; rogue state actor	

Introduction

North Korea's orientation towards creating international cybersecurity norms can be assessed by reviewing its hefty profile of major adversaries, cyberattacks, and cybersecurity policy landscape.

North Korea's attacks and unwillingness to conform could be detrimental to the shaping international cybersecurity norms. In addition to its political background, the cybersecurity strategy, cybersecurity policy landscape, international internet governance perspective, and attitudes towards agreement with the US seen within North Korea implies that North Korea to joining any agreements in the future is unlikely. Table 1.1 summarizes the findings of this case study.

Background

North Korea, also known as the Democratic People's Republic of Korea (DPRK), is a major player in the cybersecurity world because of their unwillingness to conform and their propensity for attacking using cyberweapons.

Sociopolitical Vulnerabilities

North Korea started to develop their cybercapabilities when Kim Jong Il came into power (Stent, 2018). The DPRK economy slowed and could not pay back the loans borrowed from European countries in the 1970s, causing them to no longer extend credit to North Korea (Armstrong, 2013). Continued lack of loans and constant need for hard currency for many years, led to the cybersecurity program starting in Pyongyang in the 90s, which gained speed in the early 2000s (Jun, et al., 2015).

North Korea is unique in the fact that it is a rogue actor. Its status as a rogue nation gives the DPRK advantages, such as being unbound by many conventional rules; however, rogue status comes with significant disadvantages as well (Jun, et al., 2015). North Korea is highly dependent on resources from outside countries, particularly China, and its status as an international pariah makes even its relationship with China tenuous (Albert, 2018). There is a large amount of vulnerability in being dependent on another country.

North Korea also holds great animosity towards the US starting post-WWII. Due to the US's interference in Korea after Japan's colonial rule, North Korea will likely oppose what the US attempts to accomplish for the sole reason of defying the US (Armstrong, 2013).

Level of Connectivity

The ITU site has no data on the percentage of households with a computer or households with internet access at home, but it is likely extremely close to zero, and the percentage of people using the internet is zero (International Telecommunication Union, 2017). The DPRK is highly disconnected from the rest of the world.

Major Actors in Offensive Strategy

Given the extensive profile of attacks attributed to North Korea, this report provides a discussion of major actors that play an important role in the country's offensive strategy, as opposed to a discussion of its major threat actors. There are three groups that are outside the immediate

connection to the North Korean government, but are suspected to be working with or for the DPRK government, which are the Lazarus group, APT37, and APT38 (Fraser, et al., 2018). There is another group that is acknowledged by the DPRK as part of the army—Bureau 121 (Fraser, et al., 2018). All four groups are highly disciplined and are expected to produce results for the North Korean regime. It is suspected that North Korea uses threats and indoctrination to hold strict control over each group, but it is unknown how much control North Korea actually has over the individual groups (Kim, 2018).

The Lazarus group is a hacking group with an unknown number of members. It is recorded to have existed since 2009, but their activity spiked in 2011. It works on large scale projects and produce new strands of malware constantly. The Lazarus group's code is sophisticated and constantly changing, making it a large threat (Great, 2017).

APT37's primary mission is covert intelligence gathering in support of North Korea's strategic military, political and economic interests. It consistently targets South Korea's public and private entities, as well as uses social engineering (Advanced Persistent Threat Groups, 2018).

APT38 was noticed in 2014. It has conducted operations in more than 16 organizations in at least 13 countries, sometimes simultaneously, indicating that the group is a large, prolific operation with extensive resources (Fraser, et al., 2018). The North Korean regime-backed threat group is particularly aggressive and seem to focus on gaining currency for the DPRK.

Bureau 121 is a highly trained group of hackers in the DPRK's army. It is considered to be an elite group that is hand-picked to become hackers and trained at universities in North Korea. It is comprised of approximately 1,800 people that are recruited as young as 17 (Park, 2014).

Pattern of Attacks

North Korea's cybersecurity strategy is highly dependent on aggressive, offensive behavior, using its status as a relatively low-level target to commit attacks on a small enough scale to not incur the wrath of the bigger cybersecurity powers around the globe (Jun, et al., 2015). On top of using the strategy of maintaining low target status, North Korea uses the low internet connectivity of its country as a defense. Also, North Korea disassociates and denies any involvement with the groups performing the attacks and the attacks themselves (Jun, et al., 2015). North Korea is almost never the victim but is often the perpetrator (Ko, 2018).

North Korean attacks began for monetary purpose and has rarely strayed far from that goal (Stent, 2018). It tends to aim at the financial institutions of actors which North Korea is politically against, mostly South Korea and the US because of political tensions (Armstrong, 2013).

North Korea uses small low-level attacks during peacetime to maintain fear, gain money, and disrupt the economies it holds animosity towards (Jun, et al., 2015). The country is very strategic in how and when it uses its cyberweapons. North Korea tends to aim at countries during periods where the response of those countries is going to be more sluggish than normal, like during elections or when other issues hold the attention of said country (Jun, et al., 2015). Its attacks use the strategy of poking the bear just enough to bother it, but not enough to bring retribution on themselves.

National Cybersecurity Strategy

The DPRK has one of the smallest internet presences in the entire world and is largely disconnected (Chanlett-Avery, et al., 2017). This gives North Korea a distinct advantage in the realm of cybersecurity, as the limited and filtered internet gives North Korea a pseudo air-gapped system. The lack of connectedness is good and bad for North Korea, because although it has to deal with less available internet access, it has greater control over censorship. The disconnection also makes it difficult for outside hackers to penetrate North Korea's IT systems (Jun, et al., 2015).

Offensive Cybersecurity Strategy

The number of attacks committed by North Korea greatly outnumbers the amount of times it has been attacked (Ko, 2018). There are four major attacks that are suspected to have been committed by the DPRK starting in 2009. It is hard to be sure of North Korea's involvement because of its adamant denials, the fact that the crimes were committed by groups outside of the government, and the general difficulty of attribution for cyberattacks. However, evidence and motives point to North Korea as the perpetrator or instigator.

The first of four incidents was in July 2009 when a series of DDoS attacks was carried out on governmental, financial, and media websites. The attack was attributed to APT37. Targets included the Pentagon, the White House, and the New York Stock Exchange in the US. In South Korea, the Blue House, several banks, and news agencies were similarly attacked (Ko, 2018; Chanlett-Avery, 2017).

The Compromise of Sony Pictures Entertainment occurred in December 2014 and was thought to be in response to the film "The Interview," a comedy about the assassination of Kim Jong Un. Infiltrating the company's network, the hackers released employee information and confidential emails, and deleted much of Sony's data (Ko, 2018; Chanlett-Avery, 2017).

In February 2016, the Lazarus group accessed SWIFT Network Bank and transferred funds to controlled bank accounts—$81 million was taken from the Central Bank of Bangladesh's Federal Reserve account with attacks that followed the same pattern happening in Vietnam and Ecuador. The attack was linked to the attack on Sony, which fell victim to the same malware (Ko, 2018; Chanlett-Avery, 2017).

Wannacry (May 2017) was a self-propagating ransomware attack that infected companies and individuals worldwide with a demand of cryptocurrency to harness information. The attack used a Windows vulnerability to infect over 200,000 individuals. The attack was likely less focused on the currency, only making around $140,000 in Bitcoin, but more so focused on politics and showing the prowess of North Korean hackers (Ko, 2018; Chanlett-Avery, 2017). Table 6 provides a snapshot of other suspected, or confirmed, North Korean Attacks (Ko, 2018; Chanlett-Avery, 2017; Osborne, 2018).

Table 6: Major Attacks and Targets

Attack	*Target*	*State Affiliation*	*Motivation*
Nonghyup in 2011; Customers couldn't access funds	ROK	Yes	Terrorism
2013 attacks on ROK banks and broadcasters s	ROK	Yes	Terrorism
2017 attacks on US electric companies	USA	Not confirmed	Terrorism
2017 attacks on US, European, and East Asian energy companies	MULTIPLE	Not confirmed	Terrorism
Cryptocurrency exchanges in ROK; over millions of dollars of virtual assets stolen	ROK	Not confirmed	Monetary
Global cryptojacking to mine cryptocurrency	WORLD	Not confirmed	Monetary
Ontario rail system attack (2018); attempt to derail IT systems	CAN	Not confirmed	Terrorism
Attacks on journalists and defectors using android app malware	WORLD	Not confirmed	Terrorism

Policy Landscape

The specific laws and policies surrounding the DPRK are not well known because of the secretive nature of the North Korean government. Stated in "Military and Security Developments Involving the Democratic People's Republic of Korea." North Korea views cyberweaponry as a cost-effective, asymmetric, evasive tool that can be used without much risk of reprisal attacks. The country's networks are largely separated from the internet, and disruption of internet access would have minimal impact on its economy (Report to Congress, 2015). This speaks to the reason North Korea attacks and gives credence to its defense, while the individual policies and laws surrounding cybersecurity are unknown to the public.

The Reconnaissance General Bureau (RGB) is the major known intelligence and covert operations body within the DPRK. The control of North Korea's cybercapabilites fall under The RGB's purview. The RGB is heavily related to Bureau 121 and its potential successor, the Cyber Warfare Guidance Bureau. The RGB is undergoing reorganization and is gaining more influence than the General Staff Department (Jun, et al., 2015).

The GSD oversees military operations, including the military use of cyberweapons. It is not currently associated with direct provocations like the RGB is, but its cyberunits may be tasked with preparing disruptive attacks in support of conventional military operations. North Korea's emphasis on combined arms and mixed operations suggests that cyberunits will coordinate with or will be incorporated as elements within larger conventional military formations (Jun, et al., 2015).

Tech Industry Collaboration

North Korea has little to no collaboration with private industry. This is likely due to the idea of Juche, or self-reliance (Armstrong, 2013). There are few connections between North Korea and the outside internet. Examples of such connections are between North Korea and a large Chinese internet provider called China Unicom, a backup is Thai-North Korean venture called Star JV, and a Russian telecommunications company called TransTeleCom (Williams, 2011). Due to its lack of integration, North Korea is less likely to be tied down by the threats and rules of large companies, giving them less reason to hold back when it comes to cyberattacks.

Education

North Korea extensively educates mainly its hackers (Park and Peterson, 2014). Hackers are hand-picked and undergo significant training—often at universities in Pyongyang—and then are moved to other countries to start making money for North Korea (Park and Peterson, 2014). The education has strong indoctrination woven throughout its teachings (Park and Peterson, 2014). These aspects of North Korean hackers make them a powerful tool, especially in the hands of a rogue state like North Korea. In contrast, the population of North Korea has no education on how to mitigate hacking damage—making its country vulnerable to all kinds of population-wide hacks.

International Internet Governance

Freedom House, a website that rates nation-state freedom on various levels, gives North Korea scores that indicate the least amount of freedom (Freedom House, 2018). North Korea is highly controlling of its citizens (Freedom House, 2018), which shapes the country's stance on international internet governance. Anything that seems to condone or even promote freedom of speech is likely to be immediately rejected by North Korea. The DPRK tends to agree heavily with China because of its constant support, such as the internet provided by China, and similar political alignment (Armstrong, 2013). There is also an overlap in international action between North Korea and Iran because of their opposition to the US.

Country Orientation

North Korea disagrees with a significant amount of proposed international internet governance policies. Major reasons behind North Korean disagreement include Juche, known as the feeling that

people can and should provide for themselves; freedom of speech, as it is a strong believer in censorship; the use of cyberweapons, as much of its international income comes from cyberweapons; and rejection of the US, as US international influence makes North Korean involvement in any international agreement difficult (Armstrong, 2013) (Jun, et al., 2015) (Ko, 2018).

Behavior at International Meetings

The DPRK has never sent a representative to an Intern Governance Forum (IGF) meeting. The closest the country has come to doing so was in 2017, when Myong Hak Jong took part in the IGF meeting as an online participant (IGF 2017 Online Participants). According to the Knowledge Hub, Myong Hak Jong is part of the National Coordinating Committee for Environment in Pyongyang.

US-Case Country Agreement

North Korea is a rogue actor that has a strong aversion to anything that involves the US (Armstrong, 2013). This is the biggest barrier to any US agreements with the DPRK. Regardless of inherent distaste for the US, a conflict between foundational beliefs of North Korea and the US is also a significant factor. Examples are free speech, freedom of markets, and capitalism (Armstrong, 2013).

Interactions with the DPRK remain one of the most critical security challenges for the United States and the broader international community. North Korea's willingness to undertake provocative and destabilizing behavior, such as repeated attacks on South Korea, as well as its unwillingness to stop the creation of new weaponry position the country as a major threat actor (Report to Congress, 2015). This indicates that, barring radical changes on either side, there are little to no potential areas of agreement between the US and the DPRK.

Shaping International Norms

If nothing changes in how the US and the world interact with the DPRK, there will be continued low-intensity operations and a strong likelihood of escalation to high-intensity attacks attributed to North Korea (Jun, et al., 2015). One suggestion for the international community is to have quick response teams and a strategy for the low-intensity attacks, or possibly high-intensity attacks, that will likely come from the DPRK.

A worthwhile strategy to encourage North Korea to participate in international cybersecurity collaboration could be to incentivize cooperation. Because of the damaged state of North Korea's economy, the country may be more likely to accept an offer of trade partnerships, for example, to agree to international cooperation. The major barrier to this path is North Korea's value of self-reliance, known as Juche (Armstrong, 2013).

Major Offensive Actor: Russia

By Brooke Manning

Table 7: Summary Findings, Russia

Major Offensive Attacks	
Attributed Actor	**Actor Intent/Damages**
Russian state / hackers funded by the Russian state	2007 DDoS attacks on Estonia
Russian state / Russian Business Network	2008 DDoS attacks on Georgia
Russian state / the GRU	2015 attack on the Ukrainian power grid
Russian state / the GRU / APT 28	2016 phishing campaigns and email hacks of the DNC
Russian state / the Internet Research Agency	Disinformation campaigns in the US and Europe
Russian state	2017 NotPetya attacks
Prolific Offensive Actors	
GRU, APT 28, APT 29	
Defensive Landscape	
Private Actors	**Government Partnership**
Kaspersky	Cybersecurity firm accused of Russian intelligence ties
Internet Research Agency	Organization responsible for disinformation campaigns
Russian Business Network	Cybercrime organization tied to Russian government
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Shanghai Cooperation Organization	Mutual non-aggression and regime change
Collective Security Treaty Organization	Cybersecurity development

Introduction

Russia's orientation towards creating international cybersecurity norms can be assessed by reviewing its extensive profile of intelligence-based offensive cybersecurity strategy. Russia's preference for internet sovereignty could be helpful in shaping international cybersecurity norms, but its strategy of controlling information would not be. In addition to its political background, the cybersecurity strategy, cybersecurity policy landscape, international internet governance perspective, and attitudes towards

international agreement seen within Russia implies it is unlikely to that cooperate in creating future international cybersecurity norms. Table 7 summarizes the findings of this case study.

Background

Russia's cybersecurity strategy is influenced by its political structure, which is vertical and often echoes Soviet-era norms, with rhetoric that frames intelligence organizations as protagonists and Western countries as antagonists. This translates to methodical and devastating cyberattacks, as well as severe but sophisticated approaches to internet governance.

Sociopolitical Vulnerabilities

The organization of the Russian government has undergone intense changes, especially in the last half of the century. After the Berlin Wall fell in 1989 and the Soviet Union dissolved in 1991, Russia did begin a democratization process: Leaders, such as Yeltsin, self-identified as democrats, and practices, such as electing officials, were instated (McFaul, Petrov, & Ryabov, 2010, p. vii-viii). However, there is still a high concentration of power in the president. Putin's presidency has reaffirmed this dynamic, as he has appointed friends and security services personnel to positions of power, which many argue is a remnant of the Soviet – sometimes even the Tsarist – Era (Monaghan, 2012, p. 1-2). Although the Cold War is over, the Kremlin still pushes a narrative that frames the West as Russia's main adversary, and the idea that Russia is under siege helps reinforce a strong sense of nationalism and a respect for authority (Troianovski & Nakashima, 2018). Russia's vertical political structure, central role of intelligence agencies, and hostility towards the West all remain important themes when considering the country's cybersecurity policies and cyberattack strategies.

Level of Connectivity

Russia is relatively well connected to the internet, with almost 75% of households owning a computer, slightly over 76% of households being able to access the internet, and 76% of individuals using the internet (International Telecommunications Union, 2018). However, this level of connectivity holds less weight in the context of Russia because information and the internet are becoming increasingly controlled. Furthermore, Russia has established thorough cyberdefenses. A bill passed last year requires all Internet service providers to ensure that they can continue operate even if attacked by another state, and an experiment planned to take place this spring will temporarily disconnect Russia from the internet to test its defenses (Ingber, 2019).

Pattern of Attacks

Typically, cyberattacks that come out of Russia are politically motivated, backed by the state in some form, and serve to either retain influence over post-Soviet satellite states or to interfere in political processes by using mis/disinformation. Attacks are usually well-planned and methodically

designed, reflecting the central role of secret police and surveillance techniques. Attacks aimed at former satellite states are intended to bring them back into the sphere of Russian influence and often include an element of retribution. Furthermore, Russia's cyberattacks are becoming more sophisticated and costly. Considering Russia's investment in furthering control of the internet and producing more skillful hackers, this trend will only continue.

Major Actors in Offensive Strategy

Given the extensive profile of attacks attributed to Russia, this report provides a discussion of major actors that play an important role in the country's offensive strategy, as opposed to a discussion of its major threat actors.

Russia's main intelligence body is the Federal Security Service (FSB), essentially the descendant of the Soviet-era KGB, and the organization mainly interferes with domestic politics at the state level. The GRU is frequently regarded as the "brutish cousin" of the FSB; the organization is known as Russia's main military intelligence agency and is the main actor in cases such as the crash of the Ukrainian power grid in 2015 and the hack of the DNC in the 2016 elections (Troianovski & Nakashima, 2018).

The Russian government has two Advanced Persistent Threats (APT) attributed to it. APT28, also known as Fancy Bear or the Tsar Team, is a threat group that has been attributed to the Russian state by the cybersecurity company FireEye with another cybersecurity company known as CrowdStrike—directly associating APT28 with the GRU. APT28 targets information about geopolitical issues and intelligence that would only be useful to a government, and the group operates during the working hours consistent with Moscow and St. Petersburg (FireEye, n.d.).

Also attributed to the Russian state by FireEye is APT29, known as Cozy Bear. APT29 is one of the most advanced threat groups, targeting Western European governments and foreign policy groups, as well as taking advantage of encrypted connections and communicating infrequently. Altogether, this makes Cozy Bear extremely difficult to detect (FireEye, n.d.). Since attacks by APT29 are difficult to recognize, not much information has been gathered about this hacking group.

Aside from actors directly attributed to the Russian state, there are also actors that are technically private but are hired to work on behalf of the Russian state. The most notable of these is the Internet Research Agency (IRA), which is a St. Petersburg-based company, owned by a friend of Putin, that employs hundreds of people to create methodical disinformation campaigns on social media (Chen, 2015). One of the IRA's most notable operations was the spreading of disinformation during the US 2016 election cycle, given the rarity of the US falling victim to a cyberattacks or election manipulation (Buchanan & Sulmeyer, 2016). During the 2016 US elections, the IRA created relationships with over

100 real Americans who were involved with organizing events in the physical world, although the Americans did not know they were under Russian influence (Lee, 2018).

National Cybersecurity Strategy

Russia's main goals for cybersecurity policy are to regulate information on the internet to prevent social unrest on a domestic scale, and to rival the international influence of the West and the US. However, attribution of cyberattacks to Russia is difficult, as the lines between state-sponsored actors and non-state actors are blurred. Moreover, Russia has a precedent of trying to divert blame for cyberattacks to independent hackers, but analysts often contest this.

Offensive Cybersecurity Strategy

Although the Russian state has an overwhelming portfolio of attacks, the next four cases are best able to illustrate the nuances of Russian capabilities and motives.

In 2007, the Estonian government decided to remove a bronze statue of a Soviet soldier, a decision that Russia warned against, arguing that the removal of the statue would be a form of discrimination against the ethnic Russian population (Grassegger & Krogerus, 2017). About 25% of Estonia's population is Russian, and Russia frequently exploits launching offensives against post-Soviet states, legitimizing the action by claiming it protects their ethnic citizens from being deprived of rights. Shortly after the statue was removed, DDoS attacks (via botnets) brought critical institutions in Tallinn to a standstill, compromising government websites and Estonia's largest bank. The attack ended when Estonia severed its internet connections. This cyberattack is attributed to Russia, given it had a decisive political motive and the resources to fund an offense with enough power to force Estonia to take itself off the grid. Although this is considered one of the first acts of cyberwar, it is unclear what the US obligations would be if Estonia, a recent NATO member at the time, had invoked Article 5. The lines are blurred when it comes to the collective defense clause and cyberattacks, because there is no agreed upon definition for when cyberwar constitutes actual war (Grassegger & Krogerus, 2017).

Similarly, in 2008, tensions with Russia and its Caucus neighbor Georgia escalated over mutual claims to South Ossetia, a territory disputed because of the high number of ethnic Russians living in the area (Korns & Kastenberg, 2009). This turned into five days of armed combat, with the Russian troop movements coinciding with DDoS attacks that locked Georgian government websites (Korns & Kastenberg, 2009). Not only were Georgian websites locked, but they were sometimes redirected to images comparing the then-president of Georgia, Saakashvili, to Hitler (Moses, 2008). Although Russia denied any involvement with the attack, it looks as if the Russian Business Network, a criminal gang from St. Petersburg that could be affiliated with the Russian state, was the main actor since the methods

and patterns of attack were similar (Markoff, 2008). Without permission from the US, Georgia decided to move its critical cybersecurity infrastructure to the US, as well as Poland and Estonia, which is a move that challenges the ability of US to remain neutral in a conflict that involves cyberattacks (Korns & Kastenberg, 2009). This also shows evidence that Russia has some capability to synchronize cyberattacks with traditional, kinetic attacks, further blurring the lines of what constitutes warfare, as well as the obligations of the US in a situation such as this (Korns & Kastenberg, 2009).

In 2015, parts of the Ukrainian power grid were shut down, constituting the first cyberattack to result in a blackout, leaving 230,000 people in the dark (Zetter, 2016). Not only were power stations taken offline, but backup generators were also attacked, leaving operators in the dark as well. Furthermore, there was a telephone denial of service attack (TDoS), taking customer call centers off the grid too. Ukraine was able to recover quickly, as they reverted to manual operation to run their power stations. This attack is attributed to the GRU, since it happened shortly after Ukraine began to consider nationalizing their energy companies. Energy companies that supply Ukraine, such as Gazprom, are often owned by friends of Putin, meaning that the Russian state is highly vested in whether or not Ukraine decides to nationalize private companies. The fact that the GRU might have caused a blackout, cut power to the operators, and took down customer call centers shows a level of sophistication that is typical for Russian cyberattacks (Zetter, 2016).

The NotPetya virus of 2017, attributed to Russia, is considered to be the costliest cyberattack to date. After the virus began in Ukraine, it inflicted about $10 billion in damages worldwide (Greenberg, 2018). The virus used a combination of EternalBlue, leaked NSA software that uses Microsoft exploits, and Mimikatz, malware that affects a Microsoft vulnerability with password storage. The combination of the two meant that the virus could move incredibly fast, and even if computers had been patched for EternalBlue, Mimikatz could still infect them after passwords were accessed. The virus itself mimicked a ransomware attack, but all attempts to pay ransoms were completely futile and critical files were deleted. Although Russia targeted Ukraine with NotPetya, the virus was so powerful and it spread so quickly that it affected businesses in the US, Tasmania, and as well as a Russian state-run oil company called Rosneft. However, it is also speculated that the virus was intended to spread that rapidly as a punishment for anyone who engaged with Ukrainian businesses (Greenberg, 2018).

Russia's other notable attacks include Moonlight Maze, which is often referred to as the first major cyberoperation between states; potential targeting of breakaway regions, such as Chechnya; and major email hacks, such as those that targeted the DNC in 2016 and Macron in 2017. Furthermore, it is important to recognize that a less combative, but no less effective, method of influence is Russia's

sophisticated disinformation campaigns that aim to erode trust in democratic and governmental institutions.

Policy Landscape

As previously mentioned, the main actors in cyberattacks are typically funded or affiliated with the Russian state. Besides security services, there are other government institutions that deal with internet management and legislation: The Ministry of Telecommunications leads this sector, and the Ministry of Foreign Affairs lends support on the international scale, with the latter usually advocating for a security-driven agenda (Nocetti, 2015, p. 118-119). Russia's Security Council is also an important organization when it comes to developing agenda for internet policy. The council focuses on cybersecurity and cyberdefense, as well as effective methods for communicating these ideas to an international forum like Moscow State University's Institute for Information Issues. There is often overlap between the high-ranking positions in these organizations and direct ties with the Kremlin, and it is important to note just how top-down the power structure is in Russia (Nocetti, 2015, p. 118-119).

As for legislation, it can sometimes be difficult to pinpoint a specific set of policies that regulate the internet domestically, since Russia's oligarchical framework allows measures for control to be implemented informally. One of the Kremlin's most effective methods of controlling the internet is either through direct or indirect ownership of the internet's infrastructure, and this is accomplished through the maintenance of informal social networks that eventually weed out those not willing to cooperate with state interests (Pallin, 2016, p. 18). Another method is through data localization laws, which require that data must be stored on Russian servers before being moved elsewhere and serve as a way for the Russian government to control information and monitor dissent (Newton & Summers, 2018). The data localization laws also essentially force international corporations to pay Russia for space on its servers, which both generates income for the government and deters these corporations from expanding into Russia (Newton & Summers, 2018).

Ultimately, the control of the internet in Russia mimics that of an authoritarian regime. The controls on the internet in Russia have become increasingly strict since the Arab Spring in 2012, because the Kremlin fears that a similar large-scale revolt, organized through social media, could take place in Russia (Pallin, 2016, p. 17-19). These tensions are heightened because the internet is one way that Russian citizens can consume media that is not censored by the state, and because social media use is on the rise in Russia, especially among young people (Nocetti, 2015, p. 113; Pallin, 2016, p. 20).

Tech Industry Collaboration

In general, Russia does not favor collaboration between the government and private industry. Russia views American tech companies, such as Google, Facebook, Twitter, Apple, and Microsoft, as threats to their sovereignty, and often as part of a larger conspiracy to exert US government control on the world (Nocetti, 2015, p. 114). There have also been movements in the government to stop relying on platforms such as Gmail or Microsoft Windows, and also to move servers that hold the data of Russians onto Russian territory, or at least onto Russian domains, so that Russia is able to maintain some form of jurisdiction (Nocetti, 2015, p. 114).

In contrast, Russian cybersecurity company Kaspersky is often accused of working in collaboration with the Russian state (Perlroth & Shane, 2017). Since founder of the company Yevgeny Valentinovich Kaspersky graduated from an elite KGB school and worked as a software engineer for Soviet intelligence before moving on to found Kaspersky, the company often faces allegations that it is a front for Russian intelligence operations (Shaheen, 2017). Allegedly, Israel caught Kaspersky exploiting its anti-virus software to scan for US classified programs, and it was able to obtain classified NSA documents after an employee saved them to his home computer (Perlroth & Shane, 2017).

Education

Although Russia wants to control information available on the internet, it also wants to boost tech literacy. The GRU is now making concerted efforts to increase cyber capabilities in Russia by partnering with public schools to promote math and computer sciences (Troianovski and Nakashima, 2018), recruiting university students, and funding hacking competitions (Esch, 2018). Furthermore, Russia was the first country to introduce a domain name with non-Latin characters, which greatly improved the accessibility of the internet in Russia, especially to those who exclusively spoke Russian (Nocetti, 2015, p. 121).

International Internet Governance

When it comes to international internet governance, Russia is in favor of maintaining its own sovereignty and is opposed to the multi-stakeholder approach. Russia also will follow similar lines to those drawn in the Cold War when establishing treaties.

Country Orientation

Russia would prefer to establish a “government-to-government” system of internet governance, as opposed to one that includes NGOs, tech companies, and other non-state actors that would have an equal status and not be subject to a hierarchy; essentially, Russia can be considered an advocate for a “digital version of Westphalia” (Nocetti, 2015, p. 117). Russia often abstains from treaties or agreements that would support a multi-stakeholder method of governance.

Behavior at International Meetings

Russia has not been a signatory of either the Budapest Convention on Cybercrime in 2001 or the Paris Call for Trust and Security in Cyberspace in 2018—two major cybersecurity agreements that work to coordinate international policy towards cyberconflicts. Russia did not sign the Budapest Convention because the document was interpreted as a threat to their sovereignty. Instead, the country proposed a new United Nations Convention on Cooperation in Combating Information Crimes, which would work to further the Kremlin's control on the internet (Ignatius, 2017). The UN proposal clearly demonstrates Russia's desire to control information within its borders, as well as a reluctance to cooperate unless on its own terms.

Russia is, however, part of some regional and multinational agreements. Most notably, Russia is part of the Shanghai Cooperation Organization, which is an agreement between Russia, China, Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, India, and Pakistan, and explicitly focuses on information security in the region, and is largely considered to provide security against democratization and regime change (Ambrosio, 2008, p. 1321). Furthermore, Russia is also a part of the Collective Security Treaty Organization, which consists of Kazakhstan, Kyrgyzstan, Uzbekistan, Tajikistan, and Armenia, that originally served as a post-Soviet military alliance signed in 1992, but has increasingly focused on cybersecurity issues and has similar goals to the Shanghai Cooperation Organization. Finally, Russia is part of the cooperation between Brazil, Russia, India, China, and South Africa called BRICS. BRICS is currently unable to coordinate, given some countries advocate for multi-stakeholder governance and others, such as Russia, prefer internet sovereignty (Nocetti, 2015, p. 124).

US-Russia Alignment

The number of potential disagreements between the US and Russia outweighs the potential agreements, and there is little chance that this will change in the near future. Even though both the US and Russia advocate for internet sovereignty, this does not mean that the two countries can agree on policy. The US has largely supported their own domestic governance of the internet, whereas Russia has aimed for more international organizations, but centered on their own terms (Gady & Austin, 2010).

Besides Russia actively running disinformation campaigns to interfere with US elections, there are still more barriers to cooperation between the two states. The US advocates for free speech, including on the internet. The internet in Russia is increasingly becoming controlled by the government, with surveillance and influence campaigns becoming more common, especially to prevent social uprisings (Pallin, 2017, p. 16-17). This alone would likely be a substantial enough reason for two countries to avoid cooperation. It should also be noted that Russia resents the influence that the US

exercises in internet governance, such as the main role of the US in running the Internet Corporation for Assigned Names and Numbers, and Russia actively works to make the internet itself less centered around the West (Nocetti, 2015, p. 117-120). Ultimately, with the continued use of Cold War rhetoric in Russia that emphasizes conflict between East and West, there will continue to be a high amount of issues that stand in the way from US and Russia agreement on cyberpolicies.

Shaping International Norms

Russia will likely continue along the trajectory of increasing control of the internet domestically, as well as trying to influence international policy more effectively as well. When it comes to international policy, Russia's preferences are an emphasis on state sovereignty, a prominent role for the UN, and to be considered as an equal to the US, as opposed to a subordinate. Although Russia already exerts influence regionally, and it could create problems trying to find common ground Russia in broader policy discussions, it is necessary to include Russia in shaping international norms to prevent the country from becoming even more isolated.

Russia should not be written off as an opponent, since the country possesses strong cyberoffensives, continues to increase the damages of their attacks, and actively invests in media literacy. Russia does not show restraint when engaging in cyberattacks, and this makes the country an unstable and relatively unpredictable international actor, since currently there are no good deterrents in place to discourage such actions. Allowing Russia to help shape international norms could be the first step in easing tensions in cyberspace.

Major Offensive Actor: The United States of America

By Mardav Jain

Table 8: Summary Findings, US

Major Attacks	
Attributed Threat Actor	**Actor Intent/Damages**
Russian hackers: US 2016 election interference	Political motives
North Korea's 'WannaCry' Ransomware attack	Disruption; Financial gain
Iran attacked American financial institutions in 2012; shut down Atlanta's government in 2018.	Disruption; Financial damage
Prolific Threat Actors	
China, Russia, Iran and North Korea target US for cyberespionage, intellectual property theft and financial gain	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Cyber Information Sharing Act of 2015	Create a system for federal agencies to receive threat information from private companies.
National Cybersecurity Protection Act of 2014	National Cybersecurity and Communications Integration Center integrated within the DHS
Cybersecurity & Infrastructure Security Agency Act, 2018	Creation of the Cybersecurity and Infrastructure Security Agency (CISA) within the DHS
Government Institutions	**Notable Publications**
Department of Defense	Cybersecurity Strategy of 2018
The White House	National Cybersecurity Strategy
Industry Collaboration	**Products**
Leidos, Northrup Grumman, Booz Allen Hamilton, IBM, Hewlett Packard, General Dynamics, Dell, SAIC, CSRA, CACI, Lockheed Martin, Harris and Raytheon	Improve federal cybersecurity in three areas: defense, resilience and threat analytics
Hackerone, Synack and Bugcrowd were all awarded contracts under 'Hack the Pentagon' program of 2018	Collaborate with the tech industry, use their resources to fix vulnerabilities in the Pentagon's network
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Budapest Convention – Ratified	Pursue a common criminal policy aimed at the protection of society against cybercrime

Introduction

The United States' orientation towards creating international cybersecurity norms can be assessed by reviewing its robust profile of major adversaries and cyberattacks, complex but tough cybersecurity policy landscape, and its behavior at international meetings. US' attitudes towards internet governance would not be particularly helpful in reaching consensus on international

cybersecurity norms. In addition to its political background, the offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective seen within the US implies that they will cooperate in creating future international cybersecurity norms. Table 8 summarizes the findings of this case study.

Background

The United States of America is one of the most prominent players in the international cybersecurity arena. With rapid, global development of cybercapabilities, American preeminence in the arena is now readily being challenged by other nation-states and even individual actors.

Sociopolitical Vulnerabilities

Internationally, the US has had a tumultuous history, with many nation-states using cyberwarfare against its government and citizens. Although the US "won" the Cold War when the Soviet Union fell in 1991, Russia has regained some of its lost international influence (MacFarquhar, 2018). The US is also involved in an ongoing struggle with China due to the latter's increasing international influence, which challenges US hegemony in the international realm (CLARK, 2011). The conflict is forcing both the US and China to take a more hardline approach in dealing with the other (CLARK, 2011). Iran, too, has had longstanding conflict with the US, dating back to the CIA-orchestrated coup of Iran's democratically elected Prime Minister Muhammad Mossadegh in 1953, and the subsequent Islamic Revolution of 1979 (Allen-Ebrahimian, 2017).

Domestically, since the 2016 election, the entire country has been a victim to heightened polarization between the two warring political parties and their supporters. While the 2016 election is still undergoing investigation for collusion and interference, there is also a growing sense of worry that in such tumultuous times, nation-states such as Russia will further try to exacerbate political tension via disinformation campaigns in the future elections (Denning, 2019). This cyberespionage is dangerous to the very fabric of American democracy. Accusations of outside influence in the election process threaten to delegitimize the government and create an avenue for distrust in governmental processes to rise among the populace.

Level of Connectivity

The US has a high level of connectivity with a 7.77 Information and Communications Technology (ICT) index, ranking 29th globally (ITU, 2017). In the US, 88% of households own a computer, 87% have internet access at home, and 75.2% use internet at home (ITU, 2019).

Major Threat Actors

The US's tremendous international influence and consequential implications of its domestic politics make America a prime target for cyberespionage and disinformation campaigns. China, Russia, Iran, and North Korea have all been accused of cyberwarfare against the US.

China has conducted two major types of attacks on the US. The first type are those that target governmental institutions, as well as crucial military and research organizations for the purposes of cyberespionage (Calburn, n.d.). The second kind of attacks have been on corporate infrastructure such as the attack on Gmail in 2010, which are aimed at stealing intellectual property (Markoff, 2010). APT10 known as the "Menupass Team" has been attributed to China and has been accused of targeting engineering and aerospace firms in the US as well as governmental institutions ("Advanced Persistent Threat Groups," n.d.).

Russia has in the past attacked the US with a spear phishing campaign targeted at both the US government and the private sector. APT29 known as "Cozy Bear" is suspected to be behind these attacks (Cimpanu, 2010). Russian hackers also tried to interfere with the US Presidential elections in 2016 (Yourish & Griggs, 2018).

Most of North Korea's attacks have been ransomware attacks aimed at stealing money for the regime (Busby, 2018). The country has also used hacking to steal information from the US and as well as to thwart any criticism of Kim Jong Un and his regime in the popular media (Bing and Lynch, 2018).

Iran's attacks on the US started after US targeted Iranian Nuclear Powerplant Natanz in an attack called "Stuxnet" in 2009 (Zetter, 2014). Between 2012 and 2014, Iran was suspected of targeting many American banks and was responsible for causing millions of dollars in damages (Reichmann, 2018).

Pattern of Attacks

An overview of patterns of attacks against the US allows for a comprehensive understanding of the US's place in the world. The attacks on the US are usually meant to disrupt the normal functioning of its cities, federal institutions, and private businesses. These are usually DDoS, malware, or intellectual theft attacks perpetrated by either "lone wolf" hackers or by the aforementioned nation-state actors. However, since the 2016 Presidential election, there has also been a steep increase in mis/disinformation campaigns and hacking attempts of election infrastructure.

North Korea has regularly targeted various government and private US institutions. The first of these took place in 2009, when North Korea initiated DDoS attacks against US and South Korean networks (Denning, 2018). North Korea has also been accused of hacking Sony Pictures in 2014, just before the movie 'The Interview'—a parody about Kim Jong-Un, the Supreme Leader—was to be

released (Denning, 2018). One of their more infamous attacks was the 2017 “WannaCry” ransomware attack that spread across 150 countries including the US, and resulted in hundreds of millions of dollars of damages (“White House Says WannaCry Attack Was Carried out by North Korea - CBS News”, 2017).

Russia has also been accused multiple times of hacking US institutions. One of the most infamous Russian attacks occurred in 2016, when Russian government hackers tried to interfere and influence the results in the US Presidential elections, an accusation that was further solidified in 2018, when a group of eight American intelligence agencies including the CIA, FBI and DHS all came out together to blame Russia for meddling. The Russian government was accused of hacking the Democratic National Committee’s server, the emails of Hillary Clinton campaign advisors, and was blamed for their role in the propagation of fake news to influence the election in favor of Donald Trump (Yourish & Griggs, 2018).

Iran has also attacked US institutions in the past. The country was responsible for the attack on American financial institutions in 2012, and for shutting down Atlanta’s government in 2018 (Perlroth & Benner, 2018). The US even indicted two Iranians in November 2018 for their involvement in the “SamSam” ransomware attacks (Lynch, 2018).

National Cybersecurity Strategy

Within the last decade, the US has developed both defensive and offensive national cybersecurity strategy. Obama issued a ‘Cybersecurity Framework’ in 2014, reached an agreement with Xi Jinping in 2015 to stop economic espionage and intellectual theft, and even passed the Cyber Information Sharing Act (CISA) through Congress in 2015 (Armerding, 2017). The Cybersecurity Framework set standards for both the private and the public sector while the CISA aimed at improving sharing of threat information between the private industry and the government (Armerding, 2017).

Trump, too, released a National Cybersecurity Strategy in September 2018 (Herman, 2018). This national strategy fundamentally shifts America’s approach to addressing cybersecurity issues. While in the past, the US has dealt with cybersecurity issues by shoring up its cyberdefenses, indicting cybercriminals, and sanctioning nation-states; this new strategy argues for a more offensive position (NATIONAL CYBER STRATEGY, 2018, p.3). This document is unique due to the fact that it both explicitly accuses Russia, North Korea and Iran of conducting cyberwarfare against the US and reprimands China for economic espionage and intellectual property theft (NATIONAL CYBER STRATEGY, 2018, p.1-2).

Offensive Cybersecurity Strategy

The US Cyber Command was created in 2009 within the NSA to increase cybersecurity defenses (Pomerleau, 2018). It has since then moved to a more offensive position, especially with the release of

Trump's National Security Strategy (NATIONAL CYBER STRATEGY, 2018, p.21). The US Cyber Command has also been given more offensive powers by the Trump administration; in 2018, it was promoted to equal status with the Indo-Pacific, European, Space and Joint Special Operations conventional defense commands by the US Department of Defense, thus empowered to launch attacks against foreign countries (Burton, 2018). It was also reported in 2018, that the Cyber Command's cyberwarfare cadre was officially fully manned with around 6,000 personnel (Pomerleau, 2018).

In the Department of Defense's Cybersecurity Strategy of 2018, the DOD talks about preemptively targeting our adversaries to deter malicious cyberactivity (Department of Defense, 2018, 2). The report also emphasizes the importance of a cyberforce and called for the creation of a more lethal joint force to better combat cybersecurity issues (Department of Defense, 2018, 4). The report also talks about the need for the DOD to conduct cyberspace operations to collect intelligence and prepare military capabilities (Department of Defense, 2018, 1).

The US, while being a major target for cyberespionage, has also attacked several adversaries in the past. One of the most notable American cyberattacks is Stuxnet. The American government, in association with the Israelis, used zero-day exploits to target centrifuges at a nuclear power plant in Natanz, Iran in 2008-9 (Zetter, 2014). The attack went unnoticed for months and delayed Iran's nuclear enrichment program for up to a year. The exploit did not steal data or any information from the Iranian systems, but instead was designed specifically to cause physical damage to the centrifuges and escape detection. Stuxnet was also the first digital attack of its kind to cause physical damage. The attack may have also paved way for other nation-states to use cyberwarfare to cause physical harm to infrastructure and even to human life (Zetter, 2014).

Iran is not the only nation-state or actor that the US has targeted. The US has a long history of using cyberwarfare. Kaspersky Lab calls a hacking group within the NSA, the "Equation Group," and holds them responsible for the creation of dozens of exploits, malware, and cyberattacks – Fanny, Equation Drug, and Gray Fish are particularly infamous (Equation Group, 2015). Due to the tremendous influence that the US holds over most major cybersecurity firms, it benefits from them not attributing the US for its cyberwarfare. Equation also has ties to the Stuxnet and Flame hacking groups, which are also believed to be US government supported (Equation Group, 2015).

US attacks have very specific goals, and are only carried out after years of planning by agents in US intelligence agencies. These attacks are also widely different from smaller scale attacks by countries like North Korea and Russia, because they use zero-day exploits that the agencies like NSA have specifically stockpiled for cyberwarfare like those that were used in the Stuxnet attack (Zetter, 2014).

Policy Landscape

The nation's defense strategy has increased along with the number of cyberattacks attributed against the US. Although cybersecurity is a crucial issue, given its significant political implications, the country lacks a centralized cybersecurity federal agency with each agency managing its own risk and implementing its own security solutions (Charlet, 2018, 1). Congressional oversight on the issue is also problematic because no single congressional body has full control or overview of federal cybersecurity measures (Charlet, 2018, 2). Furthermore, it is very difficult for federal agencies to adapt to threats because the legislative requirements are spread across many bills (Charlet, 2018).

The most crucial agencies for handling cybersecurity issues in the US are the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST) and the General Services Administration (GSA) (Charlet, 2018, 10).

The OMB is responsible for the development and implementation of policies, standards and guidelines on cybersecurity (Charlet, 2018, 11). Some of its responsibilities include risk-based oversight of cybersecurity programs, implementation of adopted standards and guidelines, and working with the DHS to reduce damage caused by vulnerabilities in the federal system (Federal Information Security Modernization Act, 2014).

The DHS plays a leadership role and supports other agencies in managing cybersecurity risk. DHS also seeks to provide a "common baseline" of security, act as a hub for information sharing, and promote the widespread adoption of NIST guidelines (Charlet, 2018, 12).

NIST is primarily responsible for creating appropriate standards and guidelines pertaining to cybersecurity for non-national security federal information systems (National Institute of Standards and Technology, 2014). It also gives guidelines to other federal agencies on topics such as supply risk management, wireless protocols and electronic authentication (National Institute of Standards and Technology, 2014).

The GSA is crucial because it helps the functioning of the federal government agencies by identifying and delivering cybersecurity products and services (18F: Digital service delivery). It is also responsible for digitizing systems, improving government websites and promoting cybersecurity of connected devices (18F: Digital service delivery).

In addition to the aforementioned agencies, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA) and the Department of Defense (DOD) also contribute in ensuring the cybersecurity of the country and its citizens (Charlet, 2018, 13). The intelligence community is essential for gathering information that is required by other agencies to thwart and respond to any active

cyberthreats. The DOD and the NSA can also provide technical expertise and defensive assistance. While the FBI would lead following an attack on federal systems, the DOD and NSA are responsible for defending national security systems especially the ones that are classified (Charlet, 2018, 13).

The US government has also passed several bills to address the issue of cybersecurity. The 2014 Federal Information Security Modernization Act (FISMA 2014) was passed to update the responsibilities of the DHS and the OMB in regards to information security ("FISMA Background - Risk Management", 2016). The National Cybersecurity and Communications Integration Center was integrated within the DHS under the National Cybersecurity Protection Act of 2014 (The National Cybersecurity Protection Act, 2014). The Cybersecurity Act of 2015 via the DHS was created to incentivize information sharing between the federal government and private industry (Charlet, 2018, 8). Finally, on November 13, the House passed legislation to create the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security, and on November 16, President Trump signed it into law. This will make DHS the primary agency on civilian cybersecurity for the federal government and holds promise to detangle the complex implementation of cybersecurity in the US.

Tech Industry Collaboration

The federal government is heavily involved with private industry for its cybersecurity needs. Between 2011-2016, the US government awarded cybersecurity contract to around 7,600 companies, totaling billions of dollars (Waterman, 2017). The six biggest contractors who all had contracts worth at least a billion dollars each were: Leidos, Northrup Grumman, Booz Allen Hamilton, IBM, Hewlett Packard, and General Dynamics. Some others: Dell, SAIC, CSRA, CACI, Lockheed Martin, Harris and Raytheon, all earned contracts worth hundreds of millions of dollars in three areas of federal cybersecurity spending in defense, resilience, and threat analytics (Waterman, 2017).

In October 2018, the Department of Energy (DOE) and the Department of Homeland Security (DHS) launched the Pipeline Cybersecurity Initiative in collaboration with the Oil and Natural Gas Subsector Coordinating Council (ONG SCC). The initiative is aimed at addressing cybersecurity threats to pipelines (Federal Government and Private Sector to Collaborate through the Pipeline Cybersecurity Initiative, 2018).

The Department of Defense began a "Hack the Pentagon Program" in 2016 to collaborate with the tech industry and use their resources to fix vulnerabilities in the Pentagon's network (Dowling, 2018). Hackerone, Synack, and Bugcrowd were the new tech startups that secured the contract under this program in 2018 (Dowling, 2018). The Pentagon has also been running a competition for a $10 billion-dollar clouding contract for which big names such as Amazon, Microsoft and IBM all have applied

(Nix, 2018). The Defense Department project is known as the Joint Enterprise Defense Infrastructure (JEDI) and calls for a transition of the department's old technology. JEDI wants to update some 3.4 million users and 4 million devices to a commercial cloud, and has the potential to alter the way technology providers conduct business with the Pentagon (Nix, 2018). This contract not only signals a closer linkage between tech companies and the government, but it also shows the US government's willingness to update its outdated, vulnerable federal technology.

Education

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, seeks to form a partnership between government, academia, and the private sector. NICE aims to focus on cybersecurity education, training, and workforce development (Petrella, 2017). It further aims to fulfill its mission of increasing the number of skilled cybersecurity professionals by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation (Petrella, 2017).

International Internet Governance

Due to the conception of the internet being in the US, there exists undue Western influence on how the internet works, with ramifications that affect internet users worldwide.

Country Orientation

One of the most important internet governance organizations is the Internet Corporation for Assigned Names and Numbers (ICANN) (Sanders, 2016). ICANN is sole controller of Top-Level Domain Names to all websites worldwide and thus holds tremendous power in terms of internet governance. ICANN is a non-profit in LA which until 2016, was part of the US Department of Commerce. ICANN has raised concerns about the undue influence of the West in internet governance. China and Russia have argued that ICANN impedes on their sovereignty and have demanded that their respective governments be in charge of the domain names instead (Sanders, 2016).

Although the US has been a major supporter of consensus building through international institutions such as the United Nations (UN), its views on a multi-stakeholder model for the internet are much more complex. While the recent cyberstrategy report released by the White House might suggest the Trump administration's desire for implementing a multi-stakeholder model, a careful analysis reveals other intentions. The US is intrinsically opposed to letting China and Russia use the internet for mass surveillance of their respective populations. Though internet usage is already limited and censored in both these countries, ICANN's independence provides the citizens of these countries with an opportunity create a space for dissent and political upheaval. Political tension in these countries will

directly serve US interests by undermining the growing international influence of China and Russia. The US sees the internet as another tool for these countries to have control over their populations. Thus, while the US is open to having other countries such as China and Russia have an input in internet governance, their involvement is contingent on alignment with US views.

Behavior at International Meetings

The US has shown interest in approaching cybersecurity issues through international dialogue. In 2007, the US ratified the Budapest Convention—the first and only binding agreement which was aimed to curb international cybercrime (Budapest Convention and related standards). The US has also signed onto bilateral or regional cybersecurity agreements such as the recent US-Singapore Declaration of Intent (DOI). The declaration called for collaboration through Singapore-US Cybersecurity Technical Assistance Programme for ASEAN Member States. (Singapore and the United States sign Declaration of Intent on Cybersecurity Technical Assistance Programme, 2018).

In recent years, especially with the White House's new offensive cybersecurity strategy, the US is becoming less inclined to ratify cybersecurity treaties that might limit its ability to thwart and target its adversaries. The Paris Call for Trust and Security in Cyberspace is another step in centralizing international rules around the internet, and having basic agreement on best practices regarding proliferation of cyberwarfare and capabilities. The pact was signed by 51 countries and 130 global companies, including Microsoft. However, the US – along with China, Russia, North Korea and Iran--refused to sign the Paris Call (Shepard, 2018). US's refusal is not surprising given its recent adoption of a more offensive strategy. The US seems to be working towards not only preemptive attacks, but also attacks meant to directly hurt the institutions of Russia, China and Iran (Shepard 2018).

The most promising international cybersecurity collaboration happening currently is the informal talks that the US has been holding with China and Russia to open a discourse on these issues (Lake, 2019). The latest two-day meeting was held on January 4th, 2019 in Moscow. The group, which includes Sean Kanuck, the former US national intelligence officer for cyberissues, and John Mallery, a researcher at the Massachusetts Institute of Technology (MIT), first organized these meetings in 2016 at MIT. Since then, they have had meetings in China, France, Washington and now Moscow. While each meeting deals with a different cybersecurity topic, the overarching aim of these meetings is to build consensus among the most prolific cyberactors—the US, Russia and China—and prevent an escalation of hostilities in the cyberarena (Lake 2019).

Shaping International Norms

As previously mentioned, the US is responsible for its fair share of cyberespionage against other nation-states. Despite recent changes in the international arena and inward-looking changes to US foreign policy, the country still has a stake in influencing policy decisions using cyberwarfare. For much of the 20th century, the US tried to control and influence discourse in much of Latin America—providing financial support US loyalists, and installing friendly dictators to maintain their sphere of influence (Shane, 2018). As the political opinion on such intervention has become more critical, the internet has provided the federal government with an avenue to influence domestic policy inside the borders of its new adversaries – all without accusations of imperialism. The US will also actively try to argue for a multi-stakeholder model and insist that this remain continent on alignment with US views. This will obviously be opposed by nation-states like China, Russia and Iran who prefer internet sovereignty. Thus, any ideal internet governance agreement between the US and its rival nation-states will be hard to achieve.

Despite the disinterest that major actors like the US, China and Russia have shown in establishing a general cybersecurity framework, it is essential that they join the overarching conversation on international cybersecurity norms in some capacity. The best way forward is through the informal talks that have been happening between these nation-states. These meetings are crucial for any hope of agreement and collaboration among these countries in the area of cybersecurity. By attracting vital cybersecurity experts, these meetings are creating a space for discourse to generate and for countries to find common ground (Lake, 2019).

Major Actor: Brazil

By Nicola Kalderash

Table 9: Summary Findings, Brazil

Major Attacks	
Attributed Threat Actor	**Actor Intent and Actions**
Cybercriminals	Financial gain
Prolific Threat Actors	
Cybercriminals that sought/seeking financial gain from common citizens/private sector actors.	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Marco Civil da Internet	Brazilian "Internet Bill of Rights."
Government Institutions	**Notable Publications**
Ministry of Defense	None
Industry Collaboration	**Products**
None	None
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
BRICS and IBSA	N/A

Introduction

Brazil's orientation towards creating international cybersecurity norms can be assessed by reviewing its limited profile of major adversaries and cyberattacks, limited cybersecurity policy landscape, and behavior at international meetings. Brazil's world view could be particularly helpful in shaping international cybersecurity norms. In addition to its political background, offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective seen within Brazil implies that it will cooperate in creating future international cybersecurity norms as long as Brazil is treated as an equal partner in developing international agreements. Table 9 summarizes the findings of this case study.

Background

Brazil is characterized by uneven development. A large percentage of Brazilians use the internet, but digital literacy is low, making the population vulnerable to cybercrime.

Sociopolitical Vulnerabilities

Development in Brazil has been a process with many roadblocks and complete stops. Alfredo Saad-Filho argues two incidents have enabled weak development to occur. Brazil witnessed extreme growth in its GDP, but that slowed to a crawl in the early 1970s and 1980s with the two major oil shocks and the international debt crisis. That debt crisis brought to light the incompatible fiscal and monetary taxes, something that exasperated macroeconomic troubles for Brazil further, but opened the way for acceptance of political strength in a new US alliance (Saad-Filho, 2018).

Level of Connectivity

The International Development Index by the International Telecommunication Union provides the following important statistics relating to Brazilians connectivity to the internet and other telecommunications. The level of schooling for Brazil by the average Brazilian is low, yet half of every household – 50% of households – in the country owns or has access to a computer. Of those households 52.40% of households have a connection to the internet.

A staggering 59.68% of individuals use the internet in Brazil, yet its International Development Index is ranked low on the list at 66 and 67 in 2017 and 2016 respectively. Finally, keep in mind the population by last measure of Brazil is 205,230,915; a near 100,000,000 less than the United States (ICT Development Index, 2017). High internet usage coupled with a low education rate can lead to vulnerability to cybercrime. Therefore, countries such as Brazil can only benefit from further information sharing on how to keep personal details and information safe to circumvent cybercriminal activities.

Major Threat Actors

Brazil is a country that has the capability to conduct offensive cyberattacks, but chooses not to. Although a major internet power, Brazil largely remains outside of nation-state to nation-state cyberattacks. However, Brazil is a major target of cybercriminals. Cybercriminal activity runs rampant in Brazil, but these attacks are against common citizens and not the work of nation-state-affiliated groups. Relationship wise, Brazil has great relationships with all major nation-states, although according to Brazil's Ministry of Foreign Affairs, there was a time when Portugal and Brazil had a strained relationship, but both countries now are aligned in international principles, and nothing was found that indicated there was a rocky cyber-relationship between the two (Ministry of Foreign Affairs, 2011).

Pattern of Attacks

Brazil is routinely attacked by would-be cybercriminals for financial gain. These attacks follow a pattern similar to cybercrime around the world. Attacks are very common for Brazilians connected to the internet. Angelica Mari states that over 60% – or sixty-two million people – who are connected to the internet have found themselves attacked by cybercriminals. Millennials are the most frequently

targeted and these attacks resulted in an economic loss of $22 Billion in 2017. The only country with a higher ranked loss and target rate is China. Mari concludes that malicious threats are of the most premium concern to users, privacy protection surprisingly is not high on the list (Mari, 2018).

Angelia Gonzalez-Rodriguez a journalist who tracks cyberactivity reports that C&A, a Brazilian fashion chain subsidiary, suffered a cyber-attack via its gift card platform. Tecmundo estimates that approximately 36,000 people were affected by this attack. The Public Ministry of the Federal District and Territories launched an investigation soon after the attack (Rodriguez, 2018).

Edson Sierra (2018) with FireEye Labs uncovered a malicious campaign by cybercriminals targeting banks in Brazil with malware. This campaign was multi-pronged to avoid detection and continue without interruption by staff. It utilized shortened hyperlink URLs that redirected to file depositories for the HTML attachment, GitHub. After following the link, a user would download the file, executing commands for further downloads of other required files unbeknownst to the user. It then began renaming and changing extensions of functions of key files on the computer for total access to data. It evaded detection due to its ability to keep many crucial files intact (Sierra, 2018).

As is evidenced from these attacks, there are not open attacks from other nation-states, but simply common criminals looking to strike it rich

National Cybersecurity Strategy

Nearly every country has developed some form of a cybersecurity strategy and Brazil is no exception. Brazil's strategy is a combination of policy and a lack of an offensive strategy.

Policy Landscape

Shifting into the 21st century, Brazil found itself in the position of wide adaption of new protocols regarding Brazilians and the internet. In 2016, Daniel Arnaudo writes that the law Marco Civil da Internet – or Marco Civil – was passed by the legislature of Brazil. This law was former President Rouseff's achievement and despised by her successor President Temer, who sought to repeal it. The law is essentially Brazil's bill of internet civil rights. It had the largest sweeping protections of net neutrality globally. Brazil is the world's seventh largest economy and much of the traffic of Latin America flows through Brazil as many internet nodes of connectivity are present in the country. The idea that there would be such provisions as large protection of information for citizens to access with no slowdowns would be huge not only for the country, but the region (Arnaudo, 2017).

Arnaudo continues with the example of Vice-President of Facebook Latin America Daniel Dzodan being arrested. His arrest was due to the failure to comply with WhatsApp (a company owned by Facebook) releasing data to local authorities on individuals they deemed of interest. A shutdown notice

was placed on WhatsApp by local courts and overturned by higher courts on three separate occasions within a short span of time regarding the same incident. This goes against just principles of true net neutrality (Arnaudo, 2017).

As Arnaudo argues in his article, the Right to be Forgotten is a European policy. In summary, it is the believe that individuals after a period should have the right for incidents relating to them be removed from lists in search engines. However, Brazil opted to legislate that the information not just be delisted from active searches, but deleted out right. On the surface, this doesn't appear to be much different, but in Europe the information is not deleted, it is just archived. Brazil wanted full deletion, but citizens became concerned that it would be used to make dirt and corruption from public and political officials' histories unfindable by citizens (Arnaudo, 2017). It ended up being removed.

International Internet Governance

Brazil has taken a step to be a global internet leader with the Marco Civil. Examples of new policy agreements with Germany illustrate Brazil's commitment to internet governance as well as its participation in trilateral and multilateral cooperative efforts such as IBSA and BRICS. Additionally, Brazil cooperates with the US. Overall, on the global stage, Brazil and other nation-states work together.

Country Orientation

Brazil maintains a positive attitude towards international cooperation and privacy protection. In 2014, Brazil joined in cooperation with Germany on a resolution in the United Nations for the right to privacy in the digital age (Council on Foreign Relations, 2014). The resolution was in line with many major ideologies from the Marco Civil. A cornerstone of the Marco Civil is digital privacy and net neutrality, as mentioned above.

Behavior at International Meetings

Brazil as a country interacts with other countries diplomatically as evidenced by its inclusion in South-South cooperative efforts such as IBSA, or India, Brazil, and South Africa. Additionally, Brazil is a member of a larger cooperation known as BRICS, or Brazil, Russia, India, China, and South Africa. These relationships have been shown to be strengthening the ties between these countries.

US-Brazil Alignment

Although Brazil's cybersecurity strategy is defensive rather than offensive, that does not mean it will not work closely with the US. Like the US, Brazil continues to be plagued with the threat of large cyberattacks (Neutze & Nicholas, 2013). Brazil will support further alignment with US interests so long as Brazil is given a seat at the table.

Shaping International Norms

The environment of Brazil has and continues to be one full of exploitable holes for cybercriminals big and small. However, with policy such as the Marco Civil and work through IBSA and the BRICS, Brazil has become a leader in internet governance.

Additionally, it has built and continues to build strong ties with other large nation-states and actors. Brazil would support most legislation and policy based on its past behaviors that improves cybersecurity so long as its power to govern its own country is not interfered with by any major power.

Major Actor: India

By Coley Felt

Table 10: Summary Findings, India

Major Attacks	
Attributed Threat Actor	**Actor Intent/Damages**
Unknown State Actor	Government emails and UIA of India's Aadhaar hacked
Lazarus Group (North Korea)	India's Cosmos Bank hacked
Prolific Threat Actors	
Major offensive actors interfering with the intent of espionage and financial gain	
Policies, Pending, and Passed	**Protections Provided**
Information Technology Act of 2000	Address electronic commerce and cybercrime
National Cyber Security Policy of 2013	Safeguard information, combat cyberthreats
Data Protection Bill of 2018	Restrict data flows
Government Institutions	**Notable Publications**
Ministry of Electronics and Information Technology	Security and Quality Manuals
Indian Computer Emergency Response Team(CERT-In)	Annual Reports
National Critical Information Infrastructure Centre	Common Vulnerabilities and Exposures Reports
Industry Collaboration	**Products**
Digital India Initiative	Implement various e-Governance projects
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Shanghai Cooperation Organization	Enhance cooperation in addressing cyberthreats
Memorandum of Understanding- US	Promote cooperation and exchange of information
Memorandum of Understanding- IBSA	Develop framework on Information Society in ICT

Introduction

India's orientation towards creating international cybersecurity norms can be assessed by reviewing its robust profile of major adversaries and cyberattacks, insufficient cybersecurity policy landscape, and cooperative attitude at international meetings. India's policies could be helpful in shaping international norms due to its global leadership role and volume of internet users. In addition to

its political background, India's offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective implies that it will cooperate in creating future international cybersecurity norms. Table 10 summarizes this case's findings.

Background

India's unique sociopolitical background and internet connectedness will provide insight about its weaknesses and global position regarding the formation of international cybersecurity norms.

Sociopolitical Vulnerabilities

India is home to the world's largest democracy with a population of more than 1.34 billion people ("India country profile," 2018). Although it is a democratic country, India's citizens do not have the same liberties as other democracies around the world. For example, the government controls its internet strictly, relative to other nations. India's cooperation with other southern states has shaped it into a leader for fellow developing nations in the presence of major powers at international meetings.

Level of Connectivity

India's Information and Communications Technology (ICT) index is ranked 138th in the world, with an index of 3.03. Out of all the households in India, 15.2% have computers and 22.6% have internet access. Additionally, 29.6% of individuals in India are using the internet ("ITU | 2017 Global ICT Development Index," 2017). These percentages seem relatively low; however, India's booming population means these numbers are larger than the percentages make them seem. In June 2018, the Telecom Regulatory Authority of India reported 512.26 million internet subscribers ("Indian - Computer Emergency Response Team," n.d.). India's large population combined with its high volume of internet users makes it an important, yet also vulnerable actor in the world of cyberspace.

Major Threat Actors

Examining the nation-states who attack India provides a better understanding about its relative position globally. According to the Indian Computer Emergency Response Team (CERT-In), India is ranked third in terms of cyberattacks, following the US and China (Sandhu, 2018). Another CERT-In report revealed that between April-June 2018, about 35% of cyberattacks originated from China alone. China, the US, and Russia accounted for approximately 67% of cyberattacks in Indian cyberspace. It is also believed that Pakistan is using Canadian and German cyberspace to gain access to Indian cyberspace, fueling the ongoing conflict in the southeast region from different areas of the world ("China responsible for over a third of cyberattacks on official Indian sites, NSCS informed," 2018).

Pattern of Attacks

The frequency of attacks is growing in India, with espionage and financial gain being the primary incentives behind them. Between April 2017 and January 2018, over 22,000 websites were hacked, and

114 of those were government websites infected with malware ("Major Cyber Attacks on India," 2018). Financial networks are the primary target for attackers, making for one fifth of the reported cyberattacks in 2018. Government institutions, power plants, oil refineries and pipelines are popular targets as well (Sen, 2018). As the number of attacks on Indian cyberspace grows each year, and as the country furthers its digital transformation, the scope of these attacks is spreading to many industries.

India has suffered a multitude of attacks on its critical infrastructure and government agencies. Assessing more recent major attacks allows for greater awareness of the areas of interest in Indian cyberspace. In August 2018, $13.5 million was stolen from Cosmos Bank, India's oldest national bank. It was a malware attack on the switching system, which broke communication between the payment gateway and the bank. The North Korean Lazarus group is the suspected actor (Kulkarni, 2018).

India was also one of the most affected countries that witnessed the WannaCry ransomware attack in May 2017. Official reports say approximately 45,000 computers were infected, but former director of the Intelligence Bureau, P.C. Haldar, claims that the government underplayed the attack and the number was closer to 200,000 ("WannaCry impact on India under-reported," 2017). The largest attack on Indian government networks occurred in July 2012 when more than 10,000 email addresses of top government officials were hacked. This included the Office of the Prime Minister, as well as many other offices that were involved in a phishing scheme. ("Significant Cyber Incidents Since 2006," n.d.).

National Cybersecurity Strategy

An analysis of India's offensive cybersecurity strategy, policy landscape, industry collaboration, and education will provide a comprehensive overview of its cybersecurity capabilities and readiness.

Policy Landscape

Examining the policies and institutions that govern India's cyberspace is important to understanding how the country protects and controls its internet. The Information Technology Act of 2000 is the primary law in India that addresses electronic commerce and cybercrime. The law was based on the UN Model Law on Electronic Commerce 1996 ("Ministry of Electronics and Information Technology, Government of India," n.d.). The Information Technology (Amendment) Act was passed to redefine certain terms and address issues that the original bill failed to cover. An important section within this act is Section 69, which authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion ("The Information Technology (Amendment) Act," 2008).

Additionally, the 2008 IT (Amendment) Act designated the CERT-In as the national agency to deal with cybersecurity. Established in 2004, the department operates under the Ministry of Electronics and Information Technology. Its functions include the collection, analysis and dissemination of

information on cyberincidents, forecast and alerts of cybersecurity incidents, emergency measures for handling cybersecurity incidents, coordination of cyberincident response activities and many more. ("Indian - Computer Emergency Response Team," n.d.). The National Critical Information Infrastructure Protection Centre (NCIIPC) is another department created under the 2008 IT (Amendment) Act. It is designated as the national nodal agency in respect to critical information infrastructure protection ("National Critical Information Infrastructure Protection Centre, Government of India," n.d.). The National Cyber Coordination Centre (NCCC) operates under the CERT-In and is intended to screen communication metadata and coordinate the intelligence gathering activities of other agencies. The department acts as a national internet traffic monitoring entity to detect and prevent domestic or international attacks. There is currently no legal framework, and it may be violating civil liberties and human rights (Nandikotkur, 2015).

The National Cyber Security Policy 2013 is a policy framework created by the Ministry of Electronics and Information Technology. Its mission is to safeguard information and information infrastructure in the cyberarena, develop abilities to counter and prevent cyberthreats, minimize vulnerabilities and lessen the damage from these incidents through various institutional structures, actors, processes, technology and cooperation ("National Cyber Security Policy-2013," 2013). The policy focuses on security threats and vulnerability management, securing e-Governance services, protection of critical infrastructure, promotion of research and development in cybersecurity, reducing supply chain risks, creating awareness, developing public private partnerships, and international cooperation ("National Cyber Security Policy-2013," 2013). Since India does not have its own National Security Strategy, the National Cyber Security Policy 2013 exists as an isolated departmental document rather than a national level policy. The creation of a national level cybersecurity policy would better protect India against attacks and prevent them in the future.

Tech Industry Collaboration

India's current plan to digitize the country calls for many of its sectors, along with foreign industries, to collaborate in the field of cyberspace. In 2006, India launched its National e-Governance Plan to implement various e-Governance projects around the country. The project called "Digital India" involves cooperation with many private industries as it develops its digital infrastructure ("Digital India Programme," n.d.). The initiative hopes to promote growth for the nation's electronic services, devices and employment opportunities, while also strengthening electronic manufacturing within India.

Recently, India has been fighting against American technology companies inside its borders. Government officials are intending to implement tight regulations on the companies that many Indian

citizens rely on. Major tech companies like Google, Facebook and WhatsApp are central to many Indian internet users, but new regulations aimed at national growth may limit their business opportunities. For example, the Ministry of Electronics and Information Technology has asked Facebook's WhatsApp, the most-used messaging app in India, to break the encryption that keeps messages private to help law enforcement prevent crimes. (Goel, 2018).

Additionally, with critical infrastructure being primarily owned by private companies, the Indian government must take a stronger lead to secure its critical information infrastructures. While the National Critical Information Infrastructure Protection Centre is responsible for protecting these areas, a more coordinated effort between the government and private industries has been proposed through India's Public Private Partnership program. The program has launched almost 1,500 projects to better public utilities and infrastructure. ("Overview-Public Private Partnerships in India," 2018).

Education

While most government and industry members receive cybersecurity training, the general public of India does not receive adequate education about internet security for its ample amount of users. The Indian Computer Emergency Response Team provides training to bring greater security awareness within the government, public and critical sector organizations, and communication and information providers. Its website provides tips and information directed at parents, businesses, children and women to better secure their personal devices ("Indian - Computer Emergency Response Team," n.d.).

Part of the Digital India program, the Cyber Surakshit Bharat initiative aims to enhance awareness and capacity, while helping governmental departments in the process of creating a resilient IT set up. The initiative serves as a form of cybersecurity education for both public and private participants in the Digital India program as it progresses ("Cyber Surakshit Bharat Program," 2018). Additionally, the Ministry of Electronics and Information Technology is working together with the Data Security Council of India to increase training and awareness about cybercrime investigation by setting up forensic labs in major cities. As the number of internet users in India continues to expand, cybersecurity education is vital to keeping all levels of the country secure.

International Internet Governance

India's unique digital profile along with its high volume of internet users gives the country an advantage in terms of international negotiations. Also, the developing nation has played a major role in previous negotiations regarding international meetings on security.

Country Orientation

India mentions its desire to continue to develop bilateral and multi-lateral relationships with other countries in its National Cyber Security Policy of 2013. Unlike many other major digital powers,

India has not signed the Budapest Convention on Cybercrime treaty from 2001. This is likely because India was not included in the negotiation of the Convention (Seger, 2016). India also did not sign the Paris Call for Security in Cyberspace. With the absence of major states such as the US, China, and Brazil, India's choice to sign on could encourage others to join as well (Laudrain, 2018).

India has participated in the UN Group of Governmental Experts (UN GGE) process, advocating for a common understanding for state behavior in cyberspace and the adoption of confidence-building measures by states to address cyberthreats, cyberterrorism, and cybercrimes (Patil, 2018). In 2015, India announced its support for a multi-stakeholder model of ICANN, agreeing with the US. The country has gone on to encourage Russia and China to support a multi-stakeholder model of ICANN (Patil, 2018). Additionally, India is continuing its cooperation in the IBSA (India, Brazil, South Africa) Fund ("India, Brazil and South Africa Sign Agreement for Continued Contributions to the IBSA Fund," 2017). Due to its current global cooperation and support of a multi-stakeholder model for internet governance, India would likely be in favor of the creation of an international cybersecurity policy framework.

Behavior at International Meetings

At the First Committee of the UN General Assembly on Disarmament and International Security in 2018, India voted for both the Russian Federation's and the US competing resolutions, a step towards stronger relations with both the US and Russia (Hickock & Basu, n.d.). This allows India to use aspects from both approaches to form its own that benefits the region (Hickock & Basu, n.d.). In 2017, India and Australia reaffirmed their agreement at the second Australia-India Policy Dialogue. ("Australia-India Cyber Policy Dialogue," 2018). Other recent notable Joint Statements include those with Germany and Vietnam, signed in 2017 and 2016, respectively ("Comparing Cybersecurity Norms," n.d.). India has been in support of non-governmental efforts that are developing norms such as the Global Conference on Cyber Space, which it hosted in New Delhi in 2017, as well as the Global Commission on the Stability of Cyberspace (Patil, 2018). Overall, India has led the way for other southern states while also cooperating with the major powers. India would likely continue to lead the south in international negotiations without giving up its sovereignty to China, Russia, or the US.

US-India Alignment

In 2017, the India and the US renewed the Memorandum of Understanding that was first created in 2011. The agreement reflects their shared ideals, democratic practices, security and economic interests, and ideologies for cyberspace ("Framework for the U.S.-India Cyber Relationship," 2018). In 2018, another Memorandum of Understanding was signed between the US and India when the American non-profit organization, Internet Society, and the Internet Service Providers Association of

India signed mutually agreed norms for routing security. The US nonprofit in collaboration with India shows its support in securing digital infrastructure ("ISOC signs MoU with ISPAI," 2018).

Previously, the primary barrier to agreement between India and the United States would have been their competing views of multi-stakeholder versus multi-lateral models of cybersecurity agreement. However, since the announcement of its support for a multi-stakeholder environment, India has enabled further cooperation with the US (Hickock & Basu, n.d.). In 2018, India proposed its first draft of the Personal Data Protection Bill 2018, which has risen concerns coming from US tech companies. The law aims to restrict data flows while proposing that all "critical personal data" is to only be processed inside the borders of the country. India's proposed data localization law could result in disagreement amongst future US investment and business in India's digital economy (Kalra & Shah, 2018).

Another barrier to agreement between India and the US is their differing privacy standards. The US Constitution mandates freedom of speech, but Indian law guarantees the right "to freedom of speech and expression" in Article 19 of its constitution. It also allows the Indian government to limit that freedom "in the interests of the sovereignty and integrity of India" (Kamdar, 2018). India has less legal protections regarding government searches and data requests, which may hinder US cooperation.

Shaping International Norms

Throughout its digital transformation, India should expect to see frequent cyberattacks by the major powers that are China, Russia, and the US. For this reason, along with its history of international cooperation, India would be supportive of the development of international cybersecurity norms. Supporting a multi-stakeholder model, India is positioned to lead developing countries towards further international cooperation. Its strong voice will continue to play an influential role during the development of cybersecurity cooperation, especially since India does not closely align itself with China, Russia, or the US. India's data localization laws and government surveillance may pose challenges to accepting widely-shared norms, but its collaborative attitude and desire for greater protection will encourage the country to positively participate in the formation of international cybersecurity norms.

Paris Call Signatory: Canada

By Victoria O'Laughlin and Sarah Sanguinet

Table 11: Summary Findings, Canada

Major Attacks	
Attributed Threat Actor	**Actor Intent and Actions**
Chinese government-backed hackers	Espionage
Russian Junior Naval Officer	Espionage
Iranian hacking group, Cleaver	Espionage and retaliation
Canadian government employee	Cause problems for the government
Cybercriminals	Financial gain
Prolific Threat Actors	
China, Iran, and Russia conducting espionage on Canadian confidential government operations Cybercriminals seeking financial gain or destruction	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Canada's Anti-Spam Law (CASL)	Combat viruses, malware, and spyware
Canada's Criminal Code	Prohibit both using a device to interfere with a private communication without the consent of the either party, or interfering fraudulently via computer system
Personal Information Protection and Electronic Documents Act (PIPEDA) - Passed	Notifies affected individuals of data breaches and provide a detailed description of a mitigation plan
Canada's Information Technology Incident Management Plan	Government framework for cyberthreats response
Government Institutions	**Notable Publications**
The Canadian Centre for Cyber Security	National Cyber Security Strategy; National Cyber Threat Assessment
Industry Collaboration	**Products**
Canadian Election Integrity Initiative	Address Facebook's role in disinformation
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Budapest Convention - Ratified	Common cybercrime policy
Paris Call - Signatory	Common principles for securing cyberspace

Introduction

Canada's orientation towards creating international cybersecurity norms can be assessed by reviewing its limited profile of major adversaries and cyberattacks, extensive cybersecurity policy landscape, and behavior at international meetings. Canada's cybersecurity policies and international internet governance perspective could be particularly helpful in shaping international cybersecurity

norms. In addition to its political background, the offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective seen within Canada implies that they will cooperate in creating future international cybersecurity norms. Table 11 summarizes the findings of this case study.

Background

Canada has various sociopolitical issues that could be exploited by adversaries in the event of a cyberattack on Canadian infrastructure. The nation is also positioned as an increasingly influential international cybersecurity leader, giving it a unique perspective on international cybersecurity policy.

Sociopolitical Vulnerabilities

Sociopolitical issues create tension within a population - often between citizens and governments - leaving certain demographic groups particularly vulnerable to online manipulation and cyberattack. Quebec, for instance, could be an area of potential vulnerability for foreign nation-state actors to exploit, given the province's nationalist and separatist movements. Such movements greatly compromise the strength of Canada's national government. The Premier of Quebec, François Legault, has nationalistic beliefs regarding immigration which have garnered support from populist leaders such as France's Marine Le Pen (Doughtery, 2018).

Another major sociopolitical issue Canada faces is addressing the systemic oppression of aboriginal Canadians. The disparities between Native and non-Native Canadians suggest that years of prejudice against aboriginal Canadians has had long-lasting impacts on the population (Loppie & Reading, 2014). The socioeconomic tension caused by such disparities could be used by adversaries.

Level of Connectivity

Canada's Information and Communications Technology (ICT) index is 7.77 making it rank 29th globally (ITU, 2017). In Canada, 88.2% of households own a computer, 89.23% of households have Internet access, and 89.84% of individuals use the Internet (ITU, 2019). Although these statistics indicate high levels of connectivity, Canada's ICT global rank is decreasing. Canada ranks second to last among its G7 peers (Canadian Internet Registration Authority (CIRA), 2016). Connectivity in rural Canada is particularly poor, but the Canadian Radio-television and Telecommunications Commission is continuing to further close the broadband gap affecting rural areas (Canadian Radio-television and Telecommunications Commission, 2016). Despite low connectivity in rural Canada, high national levels of connectivity suggest that Canada has a large capacity for cybersecurity development.

International Cybersecurity Leadership

Canada is a world leader in science, technology, and innovation, which has in turn positioned the country a world leader in cybersecurity. The country ranks first in the G7 for academic research and

development performance, and the qualified engineer labor force in Canada is greater than in any other G7 country (Foreign Affairs Trade and Development Canada, 2018). The Canadian Trade Commissioner Service 2018 Budget includes significant investments in a Digital Research Infrastructure Strategy to harness big data (Foreign Affairs Trade and Development Canada, 2018). Strength in research and development quality, engineering training, and overall education has advanced Canada's ability to lead internationally and develop standard cybersecurity best practices.

Major Threat Actors

Canada is a historically diplomatic country and a friend to many. Its cybersecurity leadership and reputation has not stopped adversaries from conducting cyberattacks on Canada, however. Cyber espionage giant China, and briefly Russia and Iran, have conducted cyberattacks on Canada.

China's main incentive is to acquire classified government or corporate information. For instance, in 2014, Chinese government-backed hackers accessed the National Research Council (NRC)'s Canadian government networks and classified communications (Beeby, 2017). Additionally, China sponsored APT10 conducted an espionage campaign on private Canadian firms (Bronskill, 2018). The Canadian government has suspected China of attacks like these in the past, often espionage-based (Beeby, 2017; Barton, 2014).

Russian attacks are also usually espionage driven. Since the Russian state strives for hegemony in the international sphere, it is notorious for spying on other governments (Campion-Smith, 2013). In one instance, a Russian junior naval officer hacked into and spied on Canadian Forces operations, gaining access to highly classified intelligence and communications data (Campion-Smith, 2013). The security breaches inspired a remodel of Canadian security (Campion-Smith, 2013.

Iran has also sponsored cyberattacks against Canada. For example, presumably as an act of retaliation for Canada insisting on accessing Iran's aspiring private internet, the Canadian Center for Occupational Health and Safety's (CCOHS) network and passwords were compromised in 2013 (Makuch & Ling, 2015). Iranian hacking group Cleaver used phishing campaigns to hack into the CCOHS as a gateway to access and conduct espionage on government assets (Makuch & Ling, 2015).

Pattern of Attacks

As discussed above, China, Russia, and Iran have been identified as nation-states behind cyberattacks on Canada, sponsoring APTs, hackers, and cybercriminals to conduct espionage attacks (Makuch, 2016). Canada's infrastructure, government and financial institutions, and individuals have increasingly been targeted in recent years, both by nation-states and independent cybercriminals. The Communications Security Establishment (CSE) detected 4,571 cyberattacks aimed at federal critical

infrastructure in 2016 alone (Beeby, 2017), and the following year, one in five Canadian businesses fell victim to cyberattacks (Reynolds, 2018) through theft or ransom (The Daily, 2018). Attacks targeted at large businesses were twice as more common than smaller businesses (Reynolds, 2018), indicating strong cybercriminal incentive for financial gain.

One of the most severe attacks on Canada was the 2014 NRC malware attack. The NRC contains classified research and information about Canadian defense, aerospace, energy, and cybersecurity (Barton, 2014). The attacks traced back to Chinese servers, which indicates that Chinese hackers were the culprits (Barton, 2014). As a result, there was a temporary, but expensive, shutdown of the NRC, costing Canada millions of dollars (Beeby, 2017). Despite Canada's peaceful and diplomatic relations with China, this demonstrates that even amicable countries will exploit classified information for self-gain. In June 2017, China and Canada agreed to refrain from using cyberattacks to gain business information, did not address government computers (Beeby, 2017).

Insider threats cannot be disregarded, as employees within a sophisticated organization have unique access to networks. In 2012, a distributed denial of service (DDoS) attack on Quebec's government website, www.gouv.qc.ca, blocked legitimate users from the crucial online hub for two days, and the convict was identified as a skilled government employee who uploaded malware into the network (RCMP, 2014). Residents of Quebec rely on the website to find resources pertaining to health, education, employment, general rights, and much more (Government of Quebec, 2019). The DDoS attack resulted in chaos and frustration, along with a hit to the government of Quebec's reputation.

Ransomware attacks are effective in taking advantage of the uninformed. The Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) were framed in a ransomware scam. Attackers created pop-up messages that appeared to be legitimately from these government organizations (RCMP, 2014), claiming that the user's computer was "locked due to the violation of the laws of Canada" and demanded a $100 payment in bitcoin (RCMP, 2014). Uneducated, frightened individuals succumbed (RCMP, 2014). Additionally, in 2013, 2,800 individuals reported Cryptolocker ransomware incidents to the Canadian Anti-Fraud Centre (CAFC). Individual losses amounted to $15,000 (RCMP, 2014). The incident has not been attributed to a specific actor.

Another tactic used by cybercriminals to gain access to private systems is to deploy malware using botnets. Operation Clean Slate of 2013, a collaboration between the FBI and the Royal Canadian Mounted Police, identified and mitigated 80 Canadian IP addresses which deployed Citadel (RCMP, 2014). This command and control operation, developed and distributed by a Russian cybercriminal (US

Dept. of Justice, 2015), targeted financial institutions and confidential data in Canada and other countries, costing nearly $500 million in worldwide losses (RCMP, 2014).

National Cybersecurity Strategy

An analysis of Canada's policy landscape, offensive cybersecurity strategy, tech industry collaboration, and education illuminates Canada's strong cybersecurity infrastructure and preparedness.

Offensive Cybersecurity Strategy

Canada has yet to conduct major cyberattacks against another nation-state. However, Canada's Defense Policy of 2017, "Strong, Secure, Engaged," argues for the need for development of offensive military cyberweapons (National Defence, 2017). Development of offensive strategy to supplement its defensive strategy is Canada's next step. Recently-passed Government Bill C-59 encourages Canada to perform offensive, non-violent cyberattacks when necessary (House of Commons, 2018).

Policy Landscape

Canada has dedicated a set of transparent government institutions protecting citizens' security and cybersecurity. The Canadian Centre for Cyber Security was created under the country's national security infrastructure entity, the Communications Security Establishment, with the sole purpose of focusing on cyber security strategy. The Canadian Centre for Cyber Security acts as an authoritative voice for cybersecurity issues such as incident response, public awareness, and information security guidance. The Centre is comprised of experts from Public Safety Canada, the Canadian Cyber Incident Response Centre (CCIRC), Shared Services Canada, the Security Operations Centre, and the IT branch of the CSE (Communications Security Establishment, 2018). The creation of the Canadian Centre for Cyber Security exemplifies Canada's dedication to developing robust cybersecurity infrastructure and policies.

The Canadian Centre for Cyber Security announced the National Cyber Security Strategy in 2018, which is an extensive federal cybersecurity framework that outlines the importance of cybersecurity; the strategy itself which encompasses security and resilience, leadership and collaboration, and cyber innovation; and the details regarding scope and implementation of the strategy (Communications Security Establishment, 2018). The Canadian Centre for Cyber Security also announced its first National Cyber Threat Assessment in 2018, which outlined cyber threats to Canadian citizens, businesses, and critical infrastructure (Canadian Centre for Cybersecurity, 2018).

Canada's Information Technology Incident Management Plan provides a framework for responding to cyber threats to government services. The plan aims to promote government-wide awareness of cyber threats, vulnerabilities, and confirmed incidents; enhance incident response coordination within the government; mitigate the impacts of cyber incidents to the confidentiality,

integrity, and availability of government operations; and improve public trust in the government of Canada's ability to respond to cyber incidents (Treasury Board of Canada Secretariat, 2018).

Canada's most notable cybersecurity legislation includes the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's Criminal Code, and Canada's Anti-Spam Law. PIPEDA contains cybersecurity and data protection provisions regarding organization responsibility for personal information under their jurisdiction, personal information protection according to information sensitivity, and protection methods. (Wasser, Lyons, & Koczerginski, 2017). Canada's Criminal Code prohibits using a device to interfere with a private communication without authorization, or interfering fraudulently via computer system (Wasser, Lyons, & Koczerginski, 2017). Canada's Anti-Spam Law (CASL) was created to combat viruses, malware, and spyware (Wasser, Lyons, & Koczerginski, 2017).

Tech Industry Collaboration

The CSE released a report regarding Facebook's role in disinformation during the 2019 Canadian election campaign (CSE, 2018). In response, Facebook announced the Canadian Election Integrity Initiative to address the issues highlighted by the CSE. Prime Minister Justin Trudeau warned Facebook that it could potentially face strict federal regulations after noting that the Canadian Election Integrity Initiative did not meet national expectations in terms of transparency (CSE, 2018).

Education

Canada considers education to be key in the development and enhancement of cybersecurity. The Centre for International Governance defines Canada's cybersecurity strategy using a three-pillar model; one pillar being to improve online safety through **"**a combination of public education and enhanced law enforcement capabilities" (Bonnett, 2018). Long-term investments by the government for adding digital and coding education for children into curriculum will ensure that every individual within Canada receives vital digital and coding education (Dept. of Public Safety, 2018). The government also plans to fund Canadian research in cybersecurity to provide clarity about incidents, increasing the collective cybersecurity fluency of Canadians (Dept. of Public Safety, 2018).

Part of national cybereducation includes citizens being more informed of cyberincidents. As of November 1, 2018, organizations bound by the Personal Information Protection and Electronic Documents Act (Berger et al., 2018) are required to notify affected individuals of data breaches, provide a detailed description of what information was leaked, and what the organization is doing to mitigate the leak (Legislative Services Branch, 2018). This is a step toward transparency and ultimately increases awareness among individuals of how common cyberincidents are.

Increasing participation in cybersecurity workshops shows the acknowledged relevancy of cybersecurity education. One workshop is GeekWeek, a nine-day annual workshop of cybersecurity experts from various disciplines where participants can create malware detection tools, anti-ransomware tools, and botnet traffic analysis to name a few examples (GeekWeek V, 2018). It is hosted in Canada and was established in 2014 when cyberattacks began to upswing, with the goal to keep cyberspace safe (GeekWeek V, 2018).

International Internet Governance

In the new era of cyberwarfare and cybercrime, Canada has maintained their diplomatic reputation. Canada supports international internet governance and collaboration to create international cybersecurity norms. Its intention to increase international cybersecurity agreement can be inferred from its signing onto the Paris Call, and its ratification of the Budapest Convention. Its positive behavior at the 2018 G7 summit reflects their political stance towards open communication among countries.

Country Orientation

Canada, which prefers multi-stakeholder governance, advocates for international internet governance, in which security is stronger, human rights are promoted, and internet crimes are rejected (Uchill, 2018). Canada has signed on to the Paris Call, formally indicating support for an international, free, and secure internet (National Cyber Security Strategy, 2018). This is a progressive step towards the creation of international regulations for cybersecurity (Uchill, 2018).

The pressing issue of cybercrime and its potential is widely recognized among nation-states. Canada ratified the Budapest Convention in 2015 which strengthens its additional support towards international internet governance (Government of Canada, 2015). The international treaty encourages prosecution of cybercriminals and deeper investigation of cybercrime, with global backing and cooperation strengthening the movement (Government of Canada, 2015). In July 2015, the Convention had 47 ratifications (Government of Canada, 2015). As of February 2019, 62 states have ratified it (Council of Europe, 2019), reflecting the increasing urgency to combat cybercrime.

Behavior at International Meetings

Canada hosted the 2018 G7 summit in Quebec and used its G7 Presidency to showcase both its domestic and international priorities. Cybersecurity issues were discussed during the G7 Ministerial Meeting “Building a More Peaceful and Secure World,” which was chaired by Honourable Ralph Goodale, Canadian Minister of Public Safety and Emergency Preparedness. Topics discussed within the meeting included foreign election interference, cybercrime, and threats to critical infrastructure. The meeting also highlighted the interconnected, rapidly-evolving nature of cyberthreats that make creating effective cybersecurity measures difficult for policymakers. Goodale emphasized the need for enhanced

communication between major tech companies and G7 countries to combat the spread of extremism. He further suggested that Facebook, Twitter, Google, and Microsoft communicate more regularly with the G7 about proliferation of harmful information on the internet, such as political propaganda or terrorist material (Ljunggren, David, 2018).

US-Canada Alignment

The US and Canada align well in terms of cybersecurity policy development. The countries released the 2010 Canada-U.S. Action Plan for Critical Infrastructure, which aims to promote the resiliency of critical infrastructure through information sharing, data protection protocol development, and the implementation of virtual risk management infrastructure ("U.S.-Canada Cybersecurity Cooperation," 2017). The 2012 Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security also demonstrates strong US-Canada cooperation. The Cybersecurity Action Plan promotes cyber incident response collaboration, public-private sector information sharing, and public awareness campaign development ("U.S.-Canada Cybersecurity Cooperation," 2017). Both plans point towards a strong area of cybersecurity agreement between the US and Canada.

Canada is a supporter of the Paris Call, of which the US is not. This suggests that the US and Canada may have differences in international cybersecurity agreement perspectives, despite general alignment. The Canadian government has also cast a critical eye on US tech giants and their role in compromising national cybersecurity, suggesting that agreements with the US might involve stipulations regarding these tech companies. Canada's consistent skepticism of US tech companies, such as Facebook, could be a potential barrier to future US-Canada agreements.

Shaping International Norms

Together with Estonia, France, Germany, the US, and Ukraine, which all have a positive stance towards international agreements on cybersecurity, Canada prefers a multi-stakeholder approach for the creation of international cybersecurity norms. Canada understands the growing threat of cyberattacks, and that infrastructure is vulnerable to manipulation from any international location. Any nation-state's corporations, infrastructure, and individuals are at risk of these threats, and Canada agrees that international conversation, collaboration, and norms would strengthen international cybersecurity. Given its extensive policy landscape, tech industry collaboration, and strong emphasis on education initiatives, Canada will likely advocate for capacity-building when forming international cybersecurity norms. Canada's alignment with the Paris Call and Budapest Convention, along with its behavior at international meetings, indicates a future of international cybersecurity policy cooperation.

Paris Call Signatory: Estonia

By Haiyan Wang

Table 12: Summary Findings, Estonia

Major Attacks	
Attributed Threat Actor	Actor Intent and Actions
Russian-backed group, Nashi	Disable official services
Prolific Threat Actors	
The Russian government - claimed to be responsible for the 2007 cyberattacks	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
The Action Plan to Fight Cyberattacks	Protect information systems and the integrity of data; Maintain cybersecurity; Provide defensive strategy
The National Security Concept	Manage and develop public information systems and provide cybersecurity services
Government Institutions	**Notable Publications**
European Network Information Security Agency (ENISA)	Estonian National Cyber Security Strategy; The Estonia Information Society Strategy 2013
NATO Computer Emergency Response Team (CERT)	Expert groups handling cybersecurity incidents
Industry Collaboration	**Products**
The Cyber Security Council	Manage and develop public information systems and provide cybersecurity services
Estonian Defence Unit's Cyber Unit	Formal official organization which contributes to cyberdefense
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Budapest Convention - Ratified	Common cybercrime policy
Paris Call - Signatory	Common principles for securing cyberspace

Introduction

Estonia's orientation towards creating international cybersecurity norms can be assessed by reviewing its robust profile of major adversaries and cyberattacks, sophisticated defensive cybersecurity policy landscape, behavior at international meetings, and multilateral agreements. Estonia's policies could be particularly helpful in shaping international cybersecurity norms. In addition to its political background, cybersecurity policy landscape, and international internet governance perspective seen

within Estonia implies that they will cooperate in creating future international cybersecurity norms. Table 12 summarizes the findings of this case study.

Background

Estonia is a NATO country which has adopted extensive internet services and owns a digitally-advanced society. It is regarded as one of the world's most wired countries.

Sociopolitical Vulnerabilities

Estonia has successfully established a sophisticated information system and a wide range of internet services. The government spent years leading a successful project of “e-Estonia”, aiming to transform the country into a digital society (Heller, 2017). Public services, banking, economic activities and political operations have all been digitally linked (Heller, 2017). However, the widespread internet system can be a potential risk, making the society vulnerable to be cyberattacks.

Level of Connectivity

Information and communication technologies (ICTs) cover all the aspects of social life in Estonia. The recent ICT development index (IDI) shows that the majority of the population in Estonia uses the internet. According to IDI use sub-index, the percentage of individuals using the internet in 2017 was 87.24%. Particularly, 89.58% of households have a computer and 85.19% of households have internet access. In total, IDI value in 2017 was 8.14, ranked 17 globally (ITU, 2017). The high level of connectivity reflects that Estonia is a developed, wired country where individuals' social activities are supported by internet services. It can be inferred that a compromise of the internet system would lead to a huge impact on the society. Estonia once encountered such crisis when being cyberattacked in 2007.

Major Threat Actors

The Kremlin-backed youth group, Nashi, was discovered to be sponsored by Moscow to launch a DDoS attack against media that were unfriendly to the Russian government and Putin (Shachtman, 2009). The Russian government remained anonymous by employing Nashi, making it difficult to prove their involvement. As a result, the attack signified that a hostile country could create instability in a NATO country with cyberattacks, without fear of military retaliation from NATO (McGuinness, 2017).

Regardless, the Russian state is still suspected to engage in cyberattacks against NATO networks in recent years. At the end of 2015, a suspected Russia-backed hacker used a DDoS attack as a tactic to target a Baltic petrol-distribution system, aiming to cause widespread disruption in petrol deliveries (Jewkes & Vukmanovic, 2017). The tension between Russia and the West makes EU citizens concerned. According to 2017 Eurostat survey, 86% of Europeans feel that they are increasingly threatened by cybercrime (Stolton, 2018).

Pattern of Attacks

Specifically, in April 2007, Estonia underwent a remarkable cyberattack, which can be referred as the world's first information warfare event. Nashi, and therefore the Russian government, targeted Estonian organizations in cyberspace and their information systems in response to the relocation of the Bronze Soldier of Tallinn, a Soviet-era World War II memorial (Herzog, 2011). The cyberwar disrupted governmental internet operations and affected citizens' access to public infrastructure by disabling Estonian websites via DDoS attacks. Initially, attackers used relatively inept technology methods such as ping floods. They then employed more sophisticated method by using botnets, a collection of internet-connected devices infected with malicious software, to increase the volume of DDoS attacks (Rid, 2011). Specifically, Estonian citizens were unable to access online banking services, causing huge economic disruption. One Estonian bank claimed that its operating losses due to the cyberattacks were estimated to be around one million dollars (Herzog, 2011). Moreover, the DDoS attacks greatly undermined the efficiency of public service.

National Cybersecurity Strategy

The cyberwar in 2007 has led to a series of significant changes in Estonia domestically and internationally. It led to the formation of national defensive cybersecurity policies and international internet governance framework. In response to cyberattacks, Estonia has learned more techniques and skills to help develop a national cybersecurity strategy (NCSS), a national plan of action to achieve high-level of protection of cybersecurity (Luiijf et al. 2013).

Policy Landscape

The NCSS has significantly encouraged the development of cybersecurity strategies which are beneficial to social and economic progresses. In particular, the Estonian Information Society Strategy 2013 has promoted the broad use of ICT for the development of a knowledge-based society and economy (Czosseck et al. 2011). The strategy specializes in improving living standards and public services to establish a digitally-advanced society.

In July 2007 following the attacks, the Estonian government approved the Action Plan to Fight Cyber-attacks (Czosseck et al. 2011). The action plan has sought to emphasize the importance of information systems and the integrity of data, improving cybersecurity preparedness, incident response, and defensive strategy. Ultimately, it established the legal foundation to fight against cybercrime.

Moreover, the National Security Concept was introduced in May 2010, representing the second major cybersecurity policy response from the Estonian government. The policy recognized that Estonia's increasing reliance on ICT would be accompanied by more threats attributed to cyber terrorists and organized crime groups (Czosseck et al. 2011). It constitutes the legal framework of documents which

entail objective, principles, and directions regarding security policies. The National Security Concept is revised due to the changes of Estonia's cybersecurity environment and technological development, aiming to form both a legal basis for cybersecurity preparedness and an action plan to ensure Estonia's national security. Besides, the 2007 cyberwar promoted a huge change in Estonian legislative landscape. It induced legal amendments involved several areas of law related to cybersecurity, particularly criminal law and crisis management law, to maintain the security of infrastructures (Czosseck et al. 2011). Emphasizing the crucial role of the protection of critical infrastructure, Estonia bolstered the legislation environment to facilitate the improvement of information security competence.

The cyberattacks in 2007 were significant in Estonia, but also drew attention from the international community, motivating the improvement of international cybersecurity policies and promoting international cooperation in the field of cybersecurity. In terms of the cyberattacks in 2007, the Estonian government advocated for evoking Article 5 of the NATO, which states that an assault on one allied country obligates the alliance to attack the aggressor (Shackelfod, 2009). This demonstrates that cyberattacks can also be considered as a violation of state sovereignty.

Tech Industry Collaboration

The Estonian government has successfully collaborated with private organizations and sectors against cyberattacks. Confronting the cyberwar in 2007, many cybersecurity expert volunteers were encouraged to collaborate and build a network to communicate in order to tackle the challenges in cyberspace, in the best interest of national cyberdefense (Maclellan & O'Leary, 2017). Eventually, the group evolved into a formal organization called the Estonian Defence Unit's Cyber Unit. Members were experts from different public and private sectors, who were trained to address future cyberattacks and challenges. Apart from the Estonian Defence Unit's Cyber Unit, Estonia also has established official organizations regarding cybersecurity, such as the Cyber Security Council. This group works directly with the Government Security Committee and coordinates inter-agency to respond to cyber emergencies.

Additionally, one of the most important organizations is Estonian Informatics Center (EIC), which is a state agency whose main responsibilities are to manage and develop public information services and systems, and provide cybersecurity for these services and systems. In 2009, due to the National Cyber Security Strategy, the Department of Critical information infrastructure Protection (CIIP) was added to the structure of EIC (Czosseck et al. 2011). Therefore, a new department was founded for tasks including supervising risk analyses of critical information infrastructures and developing protective measures. Finally, in terms of the cooperation between the government and private sector, a sophisticated network of cybersecurity organizations has been established based on cybersecurity strategies.

Education

To become a global heavyweight in cybersecurity, Estonia emphasizes education on cybersecurity both for individuals and organizations. Estonia has adopted the comprehensive approach (CA) to create a positive cybersecurity environment (Pernik & Tuohy, 2014). CA aims to conduct interagency education and training, which play the major role in the cooperation between public and private sectors. Meanwhile, Estonia encourages schools to provide cybersecurity courses, enabling individuals to learn the related technical knowledge and be aware of cybercrimes (Cybersecurity Summer School, 2017).

International Internet Governance

Estonia has improved technical knowledge and policies, formed emergency organizations, and gained support from the international community since the 2007 attack. Estonia now plays a leading role in international cybersecurity, advocating for international internet governance.

Country Orientation

Estonia's role in the CCDCOE is to direct research, development, training, and education in defense (Investinestonia, 2017). For example, organized by CCDCOE in Tallinn, cybersecurity teams practice cyberdefense strategies by maintaining the networks and services of a fictional cyberattacked country (Investinestonia, 2017). Therefore, Estonia invests in training cybersecurity experts, signifying great support towards international internet governance.

Behavior at International Meetings

Estonia is willing to participate in international cybersecurity discussions. It holds an annual international cybersecurity conference, CyCon 2017, in the capital (Investinestonia, 2017). During the conference, cybersecurity experts are invited to make decisions regarding the global cyberdefense community. It demonstrates that the cyberdefense world is converging on Tallinn in recent years (Investinestonia, 2017). Estonia's ratification of the Budapest Convention (Convention on Cybercrime, 2001) further indicates intentions for international collaboration and cooperation.

US-Estonia Alignment

Cooperation between these nations is essential to create a good international cybersecurity environment. Estonia has signed several agreements with NATO countries to maintain the openness and security of the global internet and defend against malicious cyberattacks. Estonia and the United States both stand on the opposite side of Russia, so it is meaningful for the United States to reach an agreement with Estonia and other NATO countries to confront cyberattacks from Russia. In 2013, the United States and Estonia signed the US-Estonia Cyber Partnership Statement at the NATO meeting (The White House, 2014). The statement emphasizes the responsibility of the United States to work with

Estonia to solve cybersecurity issues, protect secure and reliable information and enhance innovations on the internet (The White House, 2014). The primary goal is to support internet freedom, prioritizing openness and contributing to the evolution of the internet (The White House, 2014).

Shaping International Norms

The cyberattacks in 2007 promoted Estonia to develop cybersecurity strategies and policies to facilitate cyberdefense and behave positively to support international cybersecurity agreements. Estonia's response to the 2007 cyberattacks and its leadership in international agreements demonstrate that Estonia understand the importance of cyberdefense and is willing to make a commitment to international meetings, collaboration, and norms to contribute to global cybermanagement. Regarding its sophisticated policy landscape, collaboration between public and private sectors, and cooperation with NATO countries, Estonia acts as a vanguard and innovator in cyberspace. Therefore, it will be likely to advocate for building international cybersecurity norms. Estonia's signature with the Paris Call and Budapest Convention suggests that it would agree to collaborate with the nations, such as Germany and France, who have a positive stance of international cybersecurity agreements. Its leadership in CCDCOE indicates that Estonia would play a key role of defending against cybercrimes and supporting international cybersecurity cooperation.

Paris Call Signatory: France

By Evan Hobbs

Table 13: Summary Findings, France

Major Attacks	
Attributed Threat Actor	**Actor Intent/Damages**
Russia's APT28/Fancy Bear	Election interference, critical infrastructure attacks
Unattributed actor	Espionage
Prolific Threat Actors	
External actors operating to destabilize France, its democratic process, and media External public actors conducting espionage operations	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
France's International Digital Strategy	Implement multi-stakeholder and open governance and guarantees the strategic autonomy of France/EU.
National Cyber Security Strategy	Respond to cybercrime, informs the public, works towards digital security for French businesses, enhances France's voice on the international stage.
Strategic Review of Cyber Defence	Features a doctrine to manage crises.
Government Institutions	**Notable Publications**
Ministry for Europe and Foreign Affairs	France's International Digital Strategy
General Secretariat, Defence & National Security	Strategic Review of Cyber Defence
French Network and Information Security Agency	Deal with IT incidents affecting sensitive institutions.
French Ministry for the Armed Forces/Cyber defense operation chain of command	Protect the networks essential to digital warfare and military operations.
French Ministry of the Interior	Combat cybercrime against national institutions and interests. Investigates and prosecutes cybercriminals.
Industry Collaboration	**Products**
Microsoft	Paris Call for Trust and Security in Cyberspace
NATO Industry Cyber Partnership (NICP)	Network defense mechanism and task force
Charter of Trust	Signatory to the Paris Peace Call
Cybersecurity Tech Accord	Signatory to the Paris Peace Call
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Paris Call for Trust and Security in Cyberspace	Common principles for securing cyberspace
Budapest Convention – Signatory	Common cybercrime policy
NATO Warsaw Summit Cyber Defence Pledge	Recognize cyberspace as a fifth domain of warfare
G7/Ise-Shima Cyber Group	Responsible State Behavior in Cyberspace
Memorandum of Understanding – South Africa	Investigative unit that focuses on cybercrime

Introduction

France's orientation towards creating international cybersecurity norms can be assessed by reviewing its extensive profile of major adversaries and cyberattacks, deeply invested cybersecurity policy landscape, and proactive behavior at international meetings. France's presentation of the Paris

Peace Call for Trust and Security in Cyberspace is just one example of its commitment to shaping international cybersecurity norms. In addition to its political background, the offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective seen within France implies that they will cooperate, and be a leader, in creating future international cybersecurity norms. Table 13 summarizes the findings of this case study.

Background

France's alliances have had both positive and negative effects on its international agenda. Historically, these alliances have benefited western nations (Sankaran, 2019). As a founding member of, and active member within, both the European Union (EU) and NATO, France has utilized international cooperation as a tool to safeguard peace and confront world problems (Moran, 2009; NATO, 2018a). France aims to continue forming alliances to reduce conflict (Ministry for Europe and Foreign Affairs, 2018). France is determined to be a leader in regulating cyberspace (Toucas, 2018).

Sociopolitical Vulnerabilities

In accordance with promoting cooperation, France's cybersecurity strategy focuses on high levels of collaboration and transparency between nations, companies, and non-governmental organizations (Ministry for Europe and Foreign Affairs, 2017). However, France will face significant barriers to achieve a legally binding version of its Paris Call (Schonhofen, 2018).

As much as the EU and NATO alliances have benefited the country, France is constrained by not only international law, but also EU and NATO laws, regulations, and decisions (NATO, 2018b). The recent migration crisis in Europe has shown the additional difficulties that arise when countries in governmental unions disagree. In the case of migration, the founding members of the EU have traditionally accepted refugees and migrants, whereas new EU member states have typically been "immigration-averse" and want to close off borders (McGuiness, 2018a). Developing domestic and international policies, subsequently, is a longer and more tedious process.

Despite emerging as a major player in the future of internet governance, France's historic alliances with Europe and North America have created symbolic barriers that continue to ostracize non-western countries who are major actors in cybersecurity (Olejnik, 2019). The Paris Call, despite now boasting over 60 signatory nations, is a framework that many countries including the United States, China, Russia, Iran, North Korea, Brazil, India, Saudi Arabia, South Africa, and Ukraine did not sign (Uchill, 2018). While France's cybersecurity infrastructure is highly capable, France's position and leverage may not be sufficient to prevent major actors from using cyberwarfare against the country (Delerue, 2018).

Level of Connectivity

According to the International Telecommunications Union's Information and Communication Technology (ITU) Index, as of 2017, France has a high percentage of households with internet access, a computer, and individuals using the internet such that it ranks 15th globally with an index value of 8.24 (ITU, 2017). 77.5% of households have a computer and 71.4% of households have internet access at home (ITU, 2018). Individuals using the internet is even higher, at 80.5% (ITU, 2018). With high percentages of technology use and internet availability in French businesses and homes, France is vulnerable to cyberattacks, but France's focus on cybersecurity should minimize these vulnerabilities.

Major Threat Actors

France's commitment to developing cybersecurity defense systems is no coincidence. In 2015, within a 24-hour period, 1,070 denial of service attacks occurred against small French businesses (CBS News, 2015). In 2016, 24,000 cyberattacks against defense targets were thwarted by the French government (BBC News, 2017). While many attacks are claimed by certain groups, analysts often find other groups responsible for those attacks. France is more often the victim of cyberattacks than the perpetrator, which is why cyberdefense is of utmost importance (CSIS, 2019). Russia, North Korea, China, Israel, and extremist groups associated with the Islamic State have targeted French institutions, businesses, and elections (Corera, 2016; Center for Strategic and International Studies, 2017).

Russia is the main actor on France's radar. While many attacks may not come directly from Russian military intelligence agencies such as the GRU, Advanced Persistent Threat 28 (APT28), also known as Fancy Bear, has targeted France (Hern, 2017). Furthermore, Russian hacking groups have targeted individuals in France "linked to a biochemical threat conference" (CSIS, 2019). Ultimately, France's concern is that they are the active target of Russian private and governmental groups.

North Korea, while not frequently targeting France directly, was connected to the WannaCry ransomware attacks in May 2017 (Chappell, 2017; Olejnik, 2019). This attack affected major French companies including Renault (France 24, 2017). While this attack had greater impacts on other countries and their industries, such as the United Kingdom's healthcare sector, France is aware of the threat posed by North Korea's cybersecurity operations (France 24, 2017; Cybersecurity Tech Accord, 2019).

China, the perpetrator of many of the world's cyberespionage operations, was identified as responsible for infiltrating France's National Defense information systems in September of 2007 and continues to pose a threat (Center for Strategic and International Studies, 2017).

Extremist groups are also of concern for France. Many attacks are often determined to be Russian responsible, however, groups such as Cyber Caliphate frequently claim responsibility

immediately following cyberattacks against France (Corera, 2016; BBC News, 2017). While false flag sabotage operations are used to initially deflect blame, the presence and capabilities of cybercrime groups with terrorist ties pose a threat to France (Toucas, 2018).

Pattern of Attacks

France has more commonly been a target than a perpetrator of cyberattacks (Center for Strategic and International Studies, 2017). Only one attack is thought to be directed from France, a cyberespionage attack in 2015 called Animal Farm (CSIS, 2019).

The most well-known cyberattack against France was that on the election campaign of Emmanuel Macron shortly before the run-off election was held in 2017 (Nossiter, 2017). APT28, also known as Fancy Bear, was found responsible for the coordinated hacking of En Marche, Macron's political party (Greenberg, 2017; Hern, 2017). The attack resulted in an email dump that appeared to aim at destabilizing Macron's support to swing the vote to Marie Le Pen, a clear favorite of the Russians. The US's National Security Agency alerted French officials of Russian activity prior to the election taking place (Greenberg, 2017). Macron's technology team had already created "false email accounts, complete with phony documents, to confuse" and misdirect attackers (Nossiter, 2017). Cyber-blurring, a counteroffensive strategy by the Macron campaign team, slowed the cyberattack, which included "a trail of evidence" pointing to the Russian government (Nossiter, 2017).

In April 2015, a historic cyberattack in France initiated by APT28 occurred which successfully destroyed the media network of TV5Monde (Center for Strategic and International Studies, 2017). TV5Monde's 12 channels were taken off air, and control of the website and social media were lost (Corera, 2016). The Cyber Caliphate, affiliated with the Islamic State, appeared to post on TV5Monde's social media accounts and took responsibility for the cyberattack (BBC News, 2017). However, this complex attack, which breached the TV5Monde system over two months before, was later determined to be achieved by Russian hackers (Corera, 2016). This attack changed the landscape for France's policy discussions regarding cybersecurity given that the attack was not built to gain information, but instead to destroy the TV network and its systems (BBC News, 2017).

In January 2011, the National Cybersecurity Agency of France, popularly known as ANSSI, determined that emails containing malware attachments had permeated to over two hundred of the Ministry's computers (BBC News, 2011). The main targets were those who were working on the G20 Summit which occurred in Paris in February 2011 (BBC News, 2011). The attack gained information from G20 documents and other economic affairs (BBC News, 2011). The director general of the French National Agency for Information Technology Security declared this as the first major attack against

France (BBC News, 2011). This attack was more alarming given that the culprits could not be conclusively identified, even after deep analysis of the attack.

The primary motivation behind cyberattacks against France is to disrupt or impact political outcomes, specific industries or companies, or to gain information. Many of those attacks take advantage of France's infrastructure and bureaucracy through DDoS attacks or the proliferation of emails with malware. However, other attacks have unclear motives, as seen from the attack on TV5Monde which left the company uncertain as to why it specifically was targeted (Corera, 2016).

National Cybersecurity Strategy

France's international digital strategy focuses on a modern, multi-stakeholder approach (Ministry for Europe and Foreign Affairs, 2017a). In preparation for cyberattacks against the country, France has developed a national cyber security strategy that began in 2015 (Ministry for Europe and Foreign Affairs, 2019). While the development of internationally agreed upon cybersecurity norms has often been facilitated by governments, the private sector has also played a key role. Industry support from major companies such as Microsoft, Google, and Facebook has resulted in innovative and comprehensive collaborations that have inspired a movement toward a more safe and collaborative cyberspace (Ministry for Europe and Foreign Affairs, 2019).

Offensive Cybersecurity Strategy

In early 2019, France's defense secretary, Florence Parly, announced France's intention to react to cyberattacks similarly to how any country would respond to being attacked with other traditional weapons (Corfield, 2019). More money is being allocated to projects, such as COMCYBER, a cyber defense operation chain of command within the French Ministry for the Armed Forces (Olejnik, 2019). While France plans to respond to cyberattacks, the offensive strategy is a bit different than it would be in non-cyberwarfare. France's view is that the best offense is a great defense, which is why cyberweapons will be a primary instrument of defense (Corfield, 2019).

France plans on utilizing is its alliances and agreements as another offensive cybersecurity strategy. By proactively creating alliances, France aims to not only increase defense cooperation, but also to decrease the number of nations that would conduct operations against them. France's Paris Peace Call for Trust and Security in Cyberspace is a great example of this. The NATO Cyber Defence Pledge of the 2016 Warsaw Summit also shows how this can function in a modernizing world, as cyberdefense was declared to be included in NATO's collective defense (NATO, 2018b).

Policy Landscape

France has most recently led the charge for international internet governance by introducing the Paris Call for Trust and Security in Cyberspace. While France was unsuccessful in convincing key

countries to sign, it was a step in a positive direction to create norms for the future of cyberspace (Sanger, 2018). The pact asks for signatories to collaborate and communicate in the best interest of protecting international cyberspace (Ministry for Europe and Foreign Affairs, 2018b).

The creation of the French Network and Information Security Agency (ANSSI) took place in 2009 in order to develop the national cyber authority in France (Ministry for Europe and Foreign Affairs, 2019). Beyond this, France's International Digital Strategy and Strategic Review of Cyber Defence were presented by France's General Secretariat for Defence and National Security (SGDSN) and Minister for Europe and Foreign Affairs, respectively, in December 2017 and February 2018 (Ministry for Europe and Foreign Affairs, 2019). These public reports are important to France's identity as a nation and cybersecurity leader aiming to increase transparency and cooperation.

Tech Industry Collaboration

France worked closely with many companies to create, present, and gain traction on the Paris Peace Call. Microsoft was key in the formation of the pact. As of January 23, 2019, 328 companies in the private sector are signatories to the Paris Peace Call (Ministry for Europe and Foreign Affairs, 2018b). This includes those in the Cybersecurity Tech Accord and the Charter of Trust (Ministry for Europe and Foreign Affairs, 2019b). France does not shy away from industry support or collaboration, as seen on their official government website (Ministry for Europe and Foreign Affairs, 2019b), which emphasizes that industry collaboration will be key to successfully tackling international cybersecurity issues.

Education

Particularly due to attacks that have successfully stolen data from government and private institutions, digital literacy and "cyber hygiene" is a focus of the French government (Ministry for Europe and Foreign Affairs, 2018b). Many government jobs require training to ensure safe technology practices. France also boasts government run task forces which focus on digital empowerment and training to not only foster safe and healthy internet habits, but also to increase digital inclusion and media literacy (ITU Digital Inclusion Division, 2018). France and its citizens are vulnerable to disinformation campaigns, yet have the capabilities to minimize societal impact by quickly confronting issues (Worldometers, 2019).

International Internet Governance

The Paris Peace Call is the most recent step in France's attempt to develop international internet governance. Key nations such as the US, China, Russia, North Korea, Iran, Brazil, and India did not sign the agreement. (Ministry for Europe and Foreign Affairs, 2019b).

Country Orientation

As one of only four countries (China, France, Germany, Russia) that have maintained membership within the UN Group of Governmental Experts (UN GGE) since its establishment in 2004,

France continues its work to push for cyber-discussions within the Charter of the United Nations (UN) (CPI, 2017). As a member of NATO, France has taken part in several defense pledges which aim to promote compliance and cooperation at an international level (Ministry for Europe and Foreign Affairs, 2018a). This includes the 2016 Cyber Defence Pledge at the Warsaw Summit which was adopted by all 28 NATO members (Ministry for Europe and Foreign Affairs, 2018a). The Group of Seven (G7), which consists of Canada, France, Germany, Italy, Japan, the UK, and the US, has also shaped French and international policy by creating norms for behavior as seen in the 2017 G7 Declaration on Responsible States Behavior in Cyberspace (Ministry for Europe and Foreign Affairs, 2019b). Within the European Union (EU), France is also part of the Organization for Security and Cooperation in Europe (OSCE). While many goals of OSCE are non-cyber related, France aims to utilize the alliance of member countries to push a cybersecurity agenda as well (Ministry for Europe and Foreign Affairs, 2019b).

Behavior at International Meetings

President Macron represented France at the Paris Peace Forum and presented the Paris Peace Call. France's commitment to cooperation as a catalyst to achieve security is stronger than ever with Macron's foreign policy strategy and the increase in nationalist tendencies throughout Europe and non-western nations. Rather than becoming isolationist, France initiates discussions and promotes transparency (Belin, 2018). Ultimately, France enables its relationships with allies and international organizations to push for an international agenda focused on cybersecurity.

US-France Alignment

France was the United States' first ally when America was gaining independence from Britain, and the relationship has been productive for the most part since (Museum of Public Relations, 2015). While tensions increased due to different perspectives on the Iraq War, challenges due to cybersecurity threats, international terrorism, human rights, and climate change (before the Trump presidency) helped reestablish productive relations (Belkin, 2018). 2008 also marked France's return to the integrated command of NATO, which has greatly benefited the United States (Moran, 2009). France and the US are also permanent members on the United Nations Security Council. Human rights and protections against cybercrime are also priorities to these countries as both nations signed and ratified the Budapest Convention (Council of Europe, 2019). Ultimately, France and the US agree on many issues that currently challenge the globe, although there are some barriers to overcome.

Barriers

Under the Trump presidency, the US did not sign the Paris Climate Agreement nor the Paris Peace Call for Trust and Security in Cyberspace (Mooney, 2018; Matsakis, 2018). Trump has identified burdens on the economy and sovereignty as reasons behind these decisions, despite these agreements

being non-binding (Mooney, 2018; Matsakis, 2018). The fact that both agreements took place at forums hosted by France cannot be overlooked; however, President Trump has shown unilateralist tendencies throughout his presidency (Belin, 2018; Laudrain, 2018). Until a new president is inaugurated on either January 20, 2021 or January 20, 2025, the US will likely continue pursuing agreements and deals that prioritize and favor the US agenda. Today, France is seeking cooperation and transparency while the United States is pursuing an "America First" agenda (Belin, 2018). Finding similarities between the "America First" agenda and France's will be difficult barriers to overcome in the near future. Given the United States' prominent international role in the cybersecurity sphere, France will continue pushing to develop cybersecurity norms, and will hope that the US will agree to the Paris Peace Call or another similar agreement at some point in the future.

Shaping International Norms

With recent French election cyberattacks, a potential shift in power within the EU given the UK's pending exit, and the US' recent unilateralist tendencies, France has positioned itself to orient future international cybersecurity norms (Greenberg, 2017). While the US continues to leverage the idea of leaving the NATO, which has the potential of significantly reshaping France's relationship with the US, President Trump spoke highly of NATO following a summit in July 2018 (Wagner, 2018). In spite of this, France's approach to sovereignty conflicts with that of the US which resulted in President Trump's absence from the 2018 Paris Peace Forum where a declaration was signed by over 50 nations (Matsakis, 2018). Ultimately, France is taking advantage of its international role and will continue pursuing international cooperation rather than nationalist predilections (Laudrain, 2018; Belin, 2018).

The France case demonstrates its proactive role in the global cybersecurity sphere. France is uniquely positioned as a member of the Global North, the West, and Europe. The Paris Peace Call for Trust and Security in Cyberspace exemplifies France's role and hope for future cybersecurity behavior and norms, particularly given the growing threat that cyberattacks pose to institutions, infrastructure, and individuals. While the United States, China, Russia, Iran, North Korea, Brazil, India, Saudi Arabia, South Africa, and Ukraine did not sign the Paris Peace Call, France is hoping that a multi-stakeholder approach will be successful in developing sustainable and fair cybersecurity practices moving forward (Ministry for Europe and Foreign Affairs, 2017). Given France's comprehensive policy landscape, involved industry collaboration, and desire for collaboration, France's advocacy for internationally agreed upon cybersecurity norms will persist.

Paris Call Signatory: Germany

By Philipp Nonnast

Table 14: Summary Findings, Germany

Major Attacks	
Attributed Threat Actor	**Actor Intent/Damages**
Russian attacks on government servers and systems	Influence parliamentary elections
National Security Agency (NSA) and US government	Spy on German politicians, industry, and citizens
Prolific Threat Actors	
Internal and external actors attack for financial gain and political destabilization	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
IT-Sicherheitsgesetz	Requirement to report cyberattacks
Das Gemeinsame Terrorabwehrzentrum (GTAZ)	Centralization of cyberdefense centers
Government Institutions	**Notable Publications**
Bundesamt für Sicherheit und Informationstechnik(BSI)	IT-Sicherheitsgesetz (First Law on cybersecurity)
Industry Collaboration	**Products**
NATO Industry Cyber Partnership (NICP)	Network defense mechanism and task force
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Paris Call for Trust and Security in Cyberspace	Develop common ground between nations
Budapest Convention	Address cyberthreats, promote global collaboration

Introduction

Germany has a robust profile of major adversaries and cyberattacks, which has informed its limited cybersecurity policy landscape. Germany plays a significant role in the international cybersecurity sphere due to its leadership in the European Union (EU) and NATO. Germany's partnership

with the US should continue in the new era of cybersecurity developing as an increasing threat. In addition to its political background, the cybersecurity strategy, cybersecurity policy landscape, international internet governance perspective, and attitudes towards agreement, implies that both Germany will cooperate in creating future international cybersecurity norms. Table 14 summarizes the findings of this case study.

Background

Germany strives to maintain its strong image, and does not aim to disrupt the trust of its people in the government (BSI, 2018). However, recent attacks have lowered such public trust. The German government also aims to advance its goal of protecting the German people by creating a baseline of stability and protection for all information services, given the country's high level of connectivity.

Sociopolitical Vulnerabilities

While the German government is increasingly more concerned and involved in cybersecurity, it has not been significantly involved in the development of cyberdefense systems. Due to this reason, the government and state was severely shocked after a cyberattack on German politicians in 2015. Personal data, such as addresses and telephone numbers of high ranking German politicians, celebrities, and journalists were leaked (Mascolo, 2019). In response, the Parliamentary Secretary of State of the Interior, Stephan Meyer, publicly demanded rapid change and development in the landscape of German cybersecurity (Mascolo, 2019). This lack of development of defensive infrastructure, highlighted by the 2015 attack, is a significant vulnerability within Germany's cybersecurity sector.

Following the discovery of the NSA surveillance scandal in Germany via Edward Snowden leaks, German citizens and officials were upset by the hidden intentions of the US, in part due to the memory of intelligence abuse during the Nazi era and the post-World War II East-German government secret police (Guardian, 2015). While this scandal blew up in the German media, evidence has been found that German agents assisted the NSA in installing operation WHARPDRIVE in fiber cables (Spiegel, 2014). According to the Spiegel, NSA agents were to grant their appreciation, in form of a thank you letter, for the assistance of the Bundesnachrichtendiesnt (BND), referring to WHARPDRIVE (2014). This secret partnership between the US and BND started following the 9/11 attacks and appears to take place mainly in the background. Subsequently, the German public was unaware and unable to learn what the BND was passing on to the US government (Spiegel, 2014). This opaque relationship continues to worry the German public, creating a lack of trust in the German government and thus a potentially exploitable vulnerability for cyberadversaries.

Level of Connectivity

In 2017, Germany's Information and Communication Index was evaluated at 8.39, which ranked 12th globally (ITU, 2017). With a total population of just over 82 million, 91.37% of German households own a computer, 90.84% have an internet connection, and 89.65% of individuals use the internet (ITU, 2017). According to the statistics from the IUT, 9 out of 10 German citizens have access to the internet. This means that the internet plays a significant role in informing individuals and shaping their minds, thus making a large percentage of German citizens vulnerable to cyberthreats.

Major Threat Actors

As shown in a German IT journal, most of the attacks launched onto Germany have their origin in Eastern Europe and Asia (Miridakis, 2019). 24% of the attacks were traced back to Russian hackers, while the majority of all attacks originate within German borders at 36% (Miridakis, 2019). An example of Russian attacks is the November 2018 cybercampaign "Snake," which was aimed to steal politician and military data, although this has been mostly ineffective (Stolton, 2018). According to Miridakis, another 18% of the victims can attribute attacks to China, followed by Japan, Eastern Europe (without Russia), and the USA, while 13% of the affected were not able to determine the origin of the attack (2019).

Pattern of Attacks

German industries have been heavily targeted by cyberattacks and the victim of cyberespionage. Three out of four chemical and pharmaceutical companies were the victims of cyberattack in the past two years, and it is assumed that another 22% have been indirectly affected (Miridakes, 2019). Based on surveys, these attacks have affected 68% of the German automobile industry, two-thirds of the machine and mechanical engineering industry, and 63% of communication and electronic business (Miridakis, 2019). These attacks have caused approximate collateral damage of 43€ billion (Miridakis, 2019).

In 2015, the German public was made aware that the US's National Security Agency (NSA) had been spying on German citizens, politicians, and companies for decades (The Guardian, 2015). The NSA referred to the surveillance under the code name "Operation WHARPDRIVE" (Die Zeit, 2016). In order to infiltrate German communication systems, the NSA accessed major fiber optic cables and routers (Die Zeit, 2016). This violation of privacy caused significant distrust amongst German citizens regarding the NSA and the US's position as a German ally. Investigators discovered that surveillance had reached as far back as the 1990s, which left many Germans uncertain about US intentions (The Guardian, 2015). As mentioned before, the issue of Germany not having centralized cybersecurity institutions, which analyze patterns and origins of attacks, makes it difficult to prevent attacks in the future. A lack of attribution

also complicates Germany's ability to mitigate future targeted attacks by foreign nation-states. (Miridakis, 2019).

National Cybersecurity Strategy

Authorities have developed cybersecurity laws to secure the development of German networks.

Policy Landscape

The major entity protecting the German State against cyberthreats is the *Bundesamt für Sicherheit und Informationstechnik* (BSI), who focuses on constructing an encrypted central government network, which will be paired with a robust and redundant architecture (BSI, 2019). According to the BSI, the multi-layer security systems are designed by commercial and individual designed systems (2019). These systems allow for the BSI to intercept 28,000 contaminated emails and over 40,000 attacks each month (BSI, 2019). While the German government acknowledges that attackers constantly develop new technology, the nation's main goal is to prepare for the attacks and react strategically (BSI, 2019). The BSI claims that Germany is not developing any systems to retaliate post attacks (2019).

In 2011, the German government published its first cybersecurity strategy, which was revived in 2015 with the law to increase the security of information technology (IT-Sicherheitsgesetz) (BSI, 2015). The policy aims to protect Germany's critical infrastructure, such as energy, water, finance, and the nutrition industry by forcing victims of cybercrime to report incidents (BSI, 2015). The BSI aims to improve the cybersecurity of corporations and citizens (BSI, 2015).

In 2019, the federal government announced the corporation with the "*Das Gemeinsame Terrorabwehrzentrum* (GTAZ), which translates into "The comprehensive Terror-Deflection-Center,", to launch a new institution to fight cyberthreats (Mascolo 2019). This new centralized institution would be under the control of the Bundesamt fuer Sicherheit und Informationstechnik (BSI), which is the only governmental institution acting as a cybersecurity authority (Mascolo, 2019). The significant change in the GTAZ will be the inclusion of the *Bundeskriminalamt* (BKA), or the Federal Criminal Police Office, which will actively investigate as a partner of the BSI (Mascolo, 2019). Currently, Germany has not created a single database, in which all cyberattacks have been recorded (Mascolo, 2019). This makes it very difficult to analyze and notice patterns of cyberattacks, limiting the options to react and prevent future threats (Mascolo, 2019).

According to the Sued-Deutsche Zeitung, Germany is heavily criticized for lagging behind in the new world, while not being able to protect its citizens and prevent economic espionage (2019). The original National Cyber-Center was established in 2011 and located in Bonn, to specifically focus on the prevention of cyberattacks. In particular, to protect the German military and government, who are

among the most common targets. While the operating experts in place are described as outstanding in their field, the structures and execution were “suboptimal” (Mascolo, 2019). For instance, last year when Russian hackers attacked the government network, the BSI was aware of the situation, but the BKA officers at the Cyber-Center were not informed.

Germany is a founding member of the EU and a formative member, shaping new policies and development. The EU has been under a lot of pressure to develop and strengthen their cybersecurity program (EU, 2018). On December 10, 2018, the EU published an agreement on the Cybersecurity Act, which was supported by the European Parliament, Council, and Commission. According to the EU, the goal of the Act is to support all of its 28-member states to prevent threats and attacks over the internet (2018). This includes a perpetual mandate for the EU Agency for Network and Information and Security (ENISA), which further enables resource allocations to the ENISA and a better system to respond to the attacks of the EU (2018). One of its main objectives is to assist countries in preparing and building their own secure network, while the ENSIA operates as an independent and centralized institution (EU, 2018).

Germany’s large industrial sector is dependent on its NATO Industry Cyber Partnership (NICP), which aims to protect the private sector and equip it with resources to defend itself (NATO, 2018). NATO is well aware of the danger of cyberattacks to its members and the possible damage it can produce (NATO, 2018). In response to this new form of hybrid warfare, NATO focuses on a comprehensive partnership among its member states to form a strong defensive and responsive task force (NATO, 2018). According to NATO, the North Atlantic Council (NAC) is in charge of leadership and the overall implementation of developing defense mechanisms (NATO, 2018). The NATO Communications and Information Agency (NCIA) is centralized together with the NATO Computer Incident Response Capability (NCIRC) in Mons, Belgium from where it operates as the main responder to cyberattacks of member states (NATO, 2018). Furthermore, NATO is working with outsiders such as the European Union (EU), the United Nations (UN) and the Organization for Security and Co-operation in Europe (OSCE) to improve results (NATO, 2018). NATO’s involvement with other organizations is free, in order to avoid unnecessary duplication of effort and work towards a common goal (NATO 2018).

However, while NATO is focused on developing defense mechanisms, the proposed plans for a cybersecurity command center have an offensive approach (Emmot, 2018). NATO plans to have fully staffed its new military command center by 2023 to be able to detect and prevent cyberattacks, while also actively launching its own attacks (Emmont, 2018). Germany is deeply involved in supporting this new center by deploying a German Air Force commander, to lead the new cybersecurity operations center (Emmont, 2018). Due to the aftermath of World War II, Germany could never justify its own

cyberattack division, although under the shared hat of NATO, they may build cyberweapons. According to Wolfgang Renner (Air Force Commander), the new cybersecurity command center will go above and beyond the protection of member states, hinting that NATO will be able to retaliate (Emmont, 2018). In other words, Germany and all other NATO members are using NATO to counteract cyberattacks from China, North Korea, and Russia (Emmont, 2018).

Tech Industry Collaboration

The EU, and thus Germany, will use the Cybersecurity Act to build a framework of credentials that will support the development and production of goods and services throughout the EU (EU, 2018). This program will include security aspects into the early part of development and is, according to the EU, the first of its kind of law system to protect internet of things devices (EU, 2018). Moreover, the Cybersecurity Act protects businesses and their products, while incentivizing corporations to expand their business and invest in the security of their goods (EU, 2018).

Education

As part of the education for German industries and the private sector, the BSI has established a national center for the prevention, detection, and reaction to cyberattacks (BSI, 2018). Together with the National IT-Center the CERT-Bund, the Computer Emergency Response Team for German Federal Institutions provides resources to consult German citizens in the case of a cyberattack (BSI, 2018). According to the BSI, the CERT is available 24/7 and provides information on damage minimization following attacks (2018).

International Internet Governance

Germany has been and will continue to be very open to international internet governance.

Country Orientation

Following the end of the Second World War, Germany has been very involved in international governance as a member of the European Union (EU) and NATO. Together with these organizations, Germany has been deeply involved in developing and creating cyberdefense on a global scale. The country relentlessly pushes for closer cooperation and an extension of rules and guidelines on the usage of the cyberspace. Unsurprisingly, Germany was among the 51 states that signed the Paris Call, while nations like the US, China, Russian, and Iran, did not. (Matsakis, 2018). Germany's alignment with the Paris Call and Budapest Convention, indicates both support for cybercriminal prosecution and international cybersecurity policy cooperation.

Behavior at International Meetings

Germany is a member of many international organizations, such as NATO, the European Union, G20, and G7. Following the restructuring of Germany following World War II, the country has been very

involved in taking a leadership role in international meetings and organizations. Since then, Germany has become the economic leader in Europe, which has only strengthened its role and power at international conferences. With the goal to consistently develop international collaboration, Germany is a highly collaborative participant at international meetings.

US-Germany Alignment

The US and Germany have worked closely on policy development for almost 70 years. In 2016, Germany was working intensely with US advisors on the US-Germany Cyber Bilateral agreement, in which both nations committed to collaborating closely against rising cyberthreats (Chowdhry, 2016).

Germany is seeking a split from US dependency in terms of cybersecurity (Shalal, 2018). The Germany is aware of its limited tech development, but will allocate significant resources to fund its own research (Shalal, 2018). German defense and interior ministers have concluded that Germany cannot be dependent on technology from countries that attack Germany, such as the US and China (Shalal, 2018).

Shaping International Norms

As a rising leader in cybersecurity development, Germany could provide valuable insight in terms of helping shape international cybersecurity policy. While Germany is decreasing its technological dependence on other nations, millions of dollars have been allocated to the German government's resource development. To maintain its international standing, Germany is very involved in the creation of international norms. Germany’s collaborative behavior and commitment to cybersecurity development are positive examples of what necessitates international cybersecurity agreement.

Swing State: South Africa

By Connor Herriford

Table 15: Summary Findings, South Africa

Major Attacks	
Attributed Threat Actor	**Actor Intent and Actions**
Israeli secret service agency, Mossad	End South Africa's boycotts; Retaliation
Anonymous hacktivist group	Published personal data of 16,000 whistle-blowers
Internal IT specialist	Financial gain
Prolific Threat Actors	
Internal (occasionally external) cybercrime actors operating for financial gain Hacktivists protesting government corruption and lack of transparency	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
National Cybersecurity Policy Framework (NCPF) - Passed	Promotion of a cybersecurity culture that subscribes to minimum cybersecurity measures
Electronic Communications and Transactions (ECT) Act	Enable and facilitate electronic communications and transactions in the public interest
African Union Convention on Cyber Security and Personal Data Protection	Provide principles and guidelines for protection of data
Government Institutions	**Notable Publications**
State Security Agency (SSA)	Public ICT Security Reports
National Cybersecurity Advisory Council (NCAC)	Documents on legislation and ICT Policy Review
State Information Technology Agency (SITA)	Annual reports
Industry Collaboration	**Products**
Symantec Internet Security Threat Report with African Union Commission Member State governments	Identify the latest trends and cybersecurity attack statistics in Africa
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Budapest Convention - Signatory	Pursue a common criminal policy aimed at the protection of society against cybercrime
Agreement on Cooperation – Iran	Investment in ICT, satellites, e-commerce, and cybersecurity
Agreement on Cooperation – Russia	Maintain international information security
Memorandum of Understanding – India (IBSA)	Develop a framework on the Information Society in the field of ICT
Memorandum of Understanding – France	Create an investigative unit that focuses on cybercrime

Introduction

South Africa's orientation towards creating international cybersecurity norms can be assessed by reviewing its limited profile of major adversaries and cyberattacks, relatively underdeveloped cybersecurity policy landscape, and presently existing bilateral and multilateral agreements. Moreover, discourses of political transition and economic recession distract the country from further advancing their cybersecurity protocols and regulatory standards. Although South Africa has introduced a National Cybersecurity Policy Framework (NCPF), it remains one of the few nationally implemented governance frameworks pertaining to cybersecurity (State Security Agency, 2015). South Africa's underwhelming presence in international cybersecurity cooperation and their strong economic relationship towards the Brazil, Russia, India, and China (BRICS) coalition implies that they will not cooperate in creating future international cybersecurity norms. Table 15 summarizes the findings of this case study.

Background

South Africa has a plethora of potentially exploitable socio-political vulnerabilities that could be exacerbated through cyberattacks. In addition, South Africa has a strong orientation to international internet governance as a result of bilateral and multilateral economic relations with China and Russia.

Sociopolitical Vulnerabilities

Given South Africa's history, following the transition out of apartheid in 1994 – social, political, and racial divisions remain highly volatile. These divisions could be potentially exploited by any actor given a motivation. The South African government has been led by the African National Congress (ANC) since 1994. Due to a closed-list proportional representation electoral system – meaning that the order of candidates elected is fixed by the party itself, and voters are not able to express a preference for a specific candidate (ACE, 2018) – the ANC has avoided operating under a coalition. As political instability increases due to corruption and an economic recession, support for the ANC has decreased (Mbatha, 2018). This threatens a governmental coalition composition – an area that may be targeted by actors attempting to prevent or promote a coalition in the 2019 elections.

Social tensions in South Africa have also been exacerbated through manipulation and disinformation. A 2018 study by the World Bank determined that South Africa has the highest national rates of income inequality (Beaubien, 2018). In South Africa, wealth is maintained by the nation's elites, which results in inequitable income dispersion and national poverty. Internal and external actors can target this cleavage and further aggravate tensions, eliciting strong emotions by falsely accusing certain social groups. For example, a misinformation campaign in 2016 pushed a highly toxic narrative of white monopoly capital – claiming that whites in South Africa had seized resources and deprived blacks of equality and jobs (Segal, 2018).

The relationship between South Africa, China, and Russia is a product of the BRICS economic coalition and may present a potential area of future exploitation. Chinese President Xi Jinping has made sufficient investments in Africa, visiting South Africa several times to forge friendships and consolidate influence with large investments (Mbatha, 2018). Relations are similar with Russia. According to President Ramaphosa's office, Ramaphosa claimed that Russia remains an important partner to South Africa, as evidenced by their support in multilateral fora and associations such as BRICS (eNCA, 2018). If the relations between South Africa and China – or between South Africa and Russia – were to show a possibility of dissolving, China and Russia may resort to cyberattacks in the form of manipulation as a method of prevention.

Level of Connectivity

South Africa's Information and Communication Technology (ICT) index is valued at 4.96, ranking 92nd globally (ITU, 2017). In South Africa, 24.39% of households own a computer, 52.96% of households have internet access, and 54% of individuals use the internet (ITU, 2017). The integration of technology in homes, government institutions, and businesses in South Africa has increased drastically in the last decade. This increase expands the potential outreach of disinformation campaigns, other forms of manipulation, and cyberattacks at large. However, the overall underdeveloped ICT index of South Africa means that individuals are getting information from sources other than the internet – increasing the importance of traditional news sources. Moreover, a lack of mobile internet means that an individual may not be able to verify consumed information prior to sharing it with their network.

Major Threat Actors

With the accelerating pace of ICT connectivity in South Africa, their vulnerability to cyberattacks only grows in frequency and severity. Cybersecurity is an emerging national security challenge for South Africa, and a number of attacks have targeted major institutions and actors (Griffiths, 2016).

South Africa faces extensive cyberthreats to enterprises and individuals – necessitating threat awareness and cyber-resilience. According to the South African Banking Risk Information Center, South Africa has the third highest number of cybercrime victims globally – losing an estimated R2.2 billion a year to attacks (IOL, 2018). In 2016, 8.8 million South Africans were victim to online cybercrime attacks (Symantec, 2016). Attribution for these attacks are commonly accredited to internal South African actors, operating primarily for financial gain (Symantec).

Aside from cybercriminals, Niekerk notes that the most prevalent perpetrator type in South Africa was found to be hacktivists, or individuals that are affiliated to online activists' groups and are politically or ideologically motivated (Niekerk, 2017). In the past, hacktivists have acted in response to

government corruption and lack of transparency, which remains one of the main catalyzing motives behind their actions. External threat actors are less common but are suspected to play a role in cybercrime operations. Symantec notes this in their 2016 report when stating that external perpetrators may have been involved in significant cybercrime cases but have not been identified (Symantec, 2016). Additionally, a news network in Qatar, Al-Jazeera, highlighted that South Africa may have been directly threatened by Israel in 2012 for supporting Palestinian liberation groups (Sapa, 2015).

Pattern of Attacks

The attacks incurred by South Africa do not have an identifiable pattern. The majority of the attacks come from cybercriminals – some internal, some external – and commonly are for financial gain of the attacking party. In the case of the Israeli attack, South Africa was targeted for its political policies and their reluctancy to engage in economic activity with Israel. Other attacks from hacktivists, primarily DDoS and privacy infringement via mass data dumps, are in retaliation for government actions.

According to Niekerk, there have been a total of 54 major incidents of cyberattacks in South Africa over the span of 23 years (1994 - end of 2016) (Niekerk, 2017). Since then, the most prominent attack that hit South Africa was WannaCry, a ransomware attack that affected South Africa more than any other African country (Mamabolo, 2017).

An example of an additional major threatened attack was attributed to the Israeli secret service agency, Mossad, on South African banks and other institutions. On June 28, 2012, then-finance minister Pravin Gordhan received an anonymous note threatening a mass cyberattack unless there was a discontinuation of the Boycott Divestments and Sanctions campaign (Sapa, 2015). This was a global campaign promoting both various forms of boycotts against Israel, including boycotts on Israeli goods and the withdrawal from economic investments in Israel (Tripp, 2013).

In 2013, hacktivist group Anonymous carried out an attack against the South African Police Service in response to the killings of 34 miners who were protesting in Marikana (Ruane, 2013). Anonymous published the personal information of 16,000 whistle-blowers as well as hundreds of police officers. This attack demonstrates the capabilities of hacktivist groups and was a major breach of security (Griffiths, 2017).

Regarding cybercrime, major attacks have been carried out for financial gain throughout the country. In 2014, an IT specialist hacked the Gautrain Management Agency's system containing banking codes, passwords, and financial details of the staff (Hosken, 2014). The attempted heist was estimated to be for up to R800 million. In 2014 an electric provider, Eskom, had its payroll system attacked via collusion with insider IT employees (Symantec, 2016). The value of potential loss was R3.5 billion.

Ultimately, there has been a plethora of cybercrime attacks like these, often carried out by internal actors. This is partly due to the lack of security capabilities, an absence of relevant legislation, and a lack of awareness of security measures by South African government, institutions, and society (Symantec, 2016).

National Cybersecurity Strategy

South Africa is in dire need of policy that mandates focus on awareness initiatives and cybercrime threat prevention. However, despite the need to address these perennial security issues, South African policymakers and other experts have long noted the lack of detailed and reliable cyberthreat information (Symantec, 2016); yet, from a policy standpoint, not much has changed.

Offensive Cybersecurity Strategy

South Africa does not have an existing offensive cybersecurity strategy nor has South Africa been attributed to any offensive cyberattacks on other nations. This may be due to their underdeveloped cybercapabilities or an absence of an offensive cybersecurity strategy division of government.

Policy Landscape

South Africa has several government institutions and national frameworks in place to address emerging and persistent cybersecurity issues. South Africa's State Security Agency operates to provide the government with intelligence on foreign and/or domestic threats that jeopardize national security. Within the State Security Agency is a national communications branch that oversees issues related to internet and Communications Technologies (ICTs), as well as several branches that focus on counter-terrorism and espionage (State Security Agency, 2019). On October 15, 2013, South Africa's Minister of Communications inaugurated the first National Cybersecurity Advisory Council. The role of the council is to advise South Africa's government on issues pertaining to cybersecurity policy (IT News Africa, 2013). Additionally, the policy framework supplied by the National Cybersecurity Advisory Council seeks to coordinate government activities on cybersecurity to ensure cooperation between government, industry, and civil society in addressing cybersecurity threats. The State Information Technology Agency operates to render an efficient ICT service to the public sector by leveraging Information Technology (IT) for government use (National Government of South Africa, 2019). These institutions attempt to ensure national security while managing ICTs and IT services.

In general, national governments operate to draft and adopt policies to address a wide range of issues that threaten to jeopardize national security (OECD, 2012). The governance of cybersecurity in South Africa is slightly unique. It is a complex federal state with a relatively developed economy, yet it has an impoverished society that lacks digital literacy (Sutherland, 2017). Due to these factors, the South

African government faces significant challenges when developing policies related to assessing cyberthreats and responding to cyberattacks. In 2012, the South African Cabinet adopted the NCPF, aimed at providing a holistic approach pertaining to the promotion of national cybersecurity measures (State Security Agency, 2015). The NCPF also attempts to set out mechanisms for coordination across government entities. At the sub-regional level, in June 2014, the African Union adopted a Convention on Cyber Security and Personal Data Protection (African Union, 2014), aiming both to provide principles and guidelines for effective protection of data and to create a safe and secure digital environment (AU Cyber Security Expert Group). However, as argued by Orji, this Convention does not provide an adequate framework for mutual assistance nor international cooperation (Orji, 2015).

Tech Industry Collaboration

Overall, South Africa has minimal industry collaboration with private and public sectors. However, South Africa does have a few noteworthy public-private partnerships. Symantec, a cyberdefense company, released a report in 2017 titled Cyber Security Trends and Government Responses in Africa that incorporated the perspectives of African Union Commission Member State governments (Symantec, 2017). In addition, a private-sector led initiative, iCode, was developed by the Internet Service Providers Association (ISPA) of South Africa, seeking to educate the public customers and instill a culture of cybersecurity (Letsiri, 2018).

Education

Digital literacy and overall awareness of a society is paramount in order to properly defend against cyberattacks (Gutzwiller, et al., 2016). Given that a large majority of South African citizens lack digital literacy, society at large remains an exposed demographic to cyberattacks. To prevent innocent users from becoming victims, intensive awareness campaigns have been launched to educate novice users on basic security guidelines (Grobler et al., 2014). As connectivity penetration continues to increase, so does the number of new, uneducated users of technology. So long as there remains an uneducated segment of society, South African infrastructure remains vulnerable to attacks – thus threatening national security. However, South Africa has been rated as the country with the highest digital literacy in Africa, according to a report released by Siemens and Deloitte (Siemens, 2017).

International Internet Governance

South Africa has limited involvement in international internet governance initiatives and commonly votes with their strongest economic partners – China and Russia. However, South Africa has also been involved in bilateral relations with France and India.

Country Orientation

Although South Africa signed the Budapest Convention, an international treaty on cybercrime, the country has yet to ratify it (Symantec, 2016). By being a signatory of the convention, it is apparent that South Africa understands the necessity for an international cybercrime treaty but has not taken full initiative to implement it through ratification. This may be due to relational positioning with countries like China and Russia.

In 2016, South Africa sided with China and Russia in voting against a United Nations resolution aimed at the promotion and protection of human rights on the internet. The resolution sought to include provisions on the investigation of attacks on bloggers, stopping member states from preventing access to information online, and the ability to shut down internet access during key moments like elections or terror attacks (Human Rights Council, 2016). Voting with China and Russia on resolutions is commonplace for South Africa due to their multilateral economic ties with the BRICS coalition. South Africa's allegiance to Russia is further accentuated by a signed cooperation agreement between Russia and South Africa on September 4, 2017, on the basis of maintaining international information security. The press release states that the agreement shows how Russia and South Africa are striving to expand bilateral cooperation in order to maintain international and national security" (The Ministry, 2018).

South Africa's additional agreements with countries other than China and Russia focus on specific issues. For example, in their Memorandum of Understanding with France, South Africa developed a cybercrime investigative unit to address the prevalence of cybercrime in South Africa (South African Gov, 2017). This may signify an opportunity for international cooperation with entities other than those belonging to BRICS. With India, South Africa agreed to cooperate on the field of ICT (Government of India, 2017). South Africa may be open to external bilateral agreements, so long as they assist in addressing perennial national issues.

Behavior at International Meetings

Although South Africa commonly votes with China and Russia on internet governance, the country does have an international presence in attending meetings and conferences for cyber-related topics. South Africa has been present in international cyberwarfare meetings; has observed the Budapest Convention; and, in accordance with the African Union, has had multiple workshops with the European Union (Press, 2018).

US-South Africa Alignment

The US and South Africa can agree upon international standards related to cybercrime prevention, as indicated by the signing of the Budapest Convention. However, it is unclear as to why South Africa has yet to ratify the convention's framework and guidelines. Furthermore, South Africa's

current cybersecurity policies suggest agreement with the US on an abundance of policy stances. This demonstrates South Africa's understanding of US viewpoints within the security policy domain, which could potentially be an area of future agreement.

Barriers

The largest present barrier for US-South Africa relations is the economic ties to the BRICS coalition – particularly to China and Russia. Since these two countries have played a vital role in assisting in South Africa's development, it would be difficult to change their relational loyalty. Furthermore, past voting tendencies on internet governance allude to the fact that South Africa may be reluctant to adopt US policies. South Africa also typically opposes multi-stakeholder engagements, and Private-Public Partnerships are relatively non-existent in IT and cybersecurity industries.

Shaping International Norms

This case demonstrates the inclinations of swing states, which have tendencies to vote with a variety of nations on different topics and draws a picture for the voting orientation of Africa at large.

Trends in South African cybersecurity appear to remain relatively consistent with the current patterns of voting with China and Russia on cyber-related aspects (under the assumption that the governmental composition does not transition to a coalition). As President Ramaphosa took office, like Zuma before him, he continued to emphasize relations with China and Russia – alluding to a lack of immediate future deviation in international cooperation on cybersecurity. A lack of deviation can be expected from other African countries as well, due to the sheer amount of economic developmental presence China and Russia have in Africa.

However, agreements such as the bilateral memorandum with France indicate that South Africa may be willing to establish international relations to address pertinent and perpetual issues such as cybercrime. Moreover, as a signatory of the Budapest Convention, South Africa demonstrates a willingness to engage in international treaties – indicating support for international cooperation on cybercrime prosecution among governments.

Victim State: Saudi Arabia

By Amy Champagne

Table 16: Summary Findings, Saudi Arabia

Major Attacks	
Attributed Threat Actor	**Actor Intent/Damages**
Iranian government and hackers	Political motives
Iranian government	Political and economic motives
Prolific Threat Actors	
Iranian government and Iranian hackers conducting attacks on Saudi government to gain political influence in the region and to test new hacking technologies	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Vision 2030	Create goals for the country to diversify the economy, through technical education and jobs
Anti-Cyber Crime Law	Outlines unlawful cybercrimes and punishments
Government Institutions	**Notable Publications**
National Cyber Security Center (NCSC)	Provide quarterly statistic reports about cyber threats and risks
Communication and Information Technology Commission (CITC)	A Comprehensive Study on The State of ICT Market Development in Saudi Arabia
Industry Collaboration	**Products**
Hacker Team	Ownership of 20% of the company to gain control on where the company should allocate resources
Investment in tech companies	Incentives for global companies to meet any demands requested by the Saudi government
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Budapest Convention – Ratified	Pursue a common criminal policy aimed at the protection of society against cybercrime
International Multilateral Partnership Against Cyber Threats (IMPACT)	Provide countries with resources and expertise to better protect against cyberthreats.

Introduction

Saudi Arabia's orientation towards creating international cybersecurity norms can be assessed by reviewing its robust profile of major adversaries and cyberattacks, limited cybersecurity policy landscape, and behavior at international meetings. Although there aren't many, Saudi Arabia's policies could be particularly helpful in shaping international cybersecurity norms. In addition to its political background, the offensive cybersecurity strategy, cybersecurity policy landscape, and international internet governance perspective seen within Saudi Arabia implies that they will cooperate in creating future international cybersecurity norms. Table 16 summarizes the findings of this case study.

Background

Saudi Arabia handles sociopolitical issues that primarily stem from a power struggle with Iran. The constant cyberattacks from Iran is not only pressuring the Saudi government to address weaknesses in the country, but is also creating justification for the government to servile citizens.

Sociopolitical Vulnerabilities

Saudi Arabia, along with Iran, is one of the major actors in the Middle East. Unlike Iran, Saudi Arabia is an ally of the US (CFR.org Editors, 2018). The US and Saudi Arabia share strong cooperation on security and trade dominated by the US's interest in Saudi oil. Saudi Arabia is a critical US ally in the Middle East, and shares a rivalry with Iran (CFR.org Editors, 2018).

The rivalry between Saudi Arabia and Iran is primarily due to a power struggle in the region (Marcus, 2017). Both countries have a majority Muslim population, but each country follows an opposing interpretation of the religion (Marcus, 2017). While Saudi Arabia is largely a Sunni Muslim country, Iran is primarily a Shia Muslim country (Marcus, 2017). Thus, surrounding countries follow the leadership of each power depending on their country's interpretation of Islam (Marcus, 2017). After Iran was targeted by the Stuxnet attack in 2010, Iran has been ramping up it cyberattack tactics, which are experimented on Saudi Arabia. Before facing major attacks from Iran, Saudi Arabia had no cyberdefense institutions and limited cybersecurity policy. Since facing threats from Iran, Saudi Arabia has ramped up efforts to strengthen cybersecurity.

Major weaknesses in Saudi Arabia are largely due to poor cybersecurity practices from individual users. While international actors are focusing their efforts on attacking government agencies, individual citizens are also under threat by spyware and other surveillance tactics by the Saudi government (Alabdulatif, 2018).

Level of Connectivity

Saudi Arabia's Information and Communication Technology (ICT) is 6.87, ranking 45th globally (ITU, 2017). In Saudi Arabia, 73% of households own a computer, 93% of households have internet access, and 82.1% of individuals use the internet (ITU, 2018). Although these numbers have dramatically increased in the last decade, Saudi Arabia's global rank is decreasing in terms of information and technology (ITU, 2017). The increasing number of individuals gaining access to the internet and smart devices poses a greater threat to individuals being targeted by blended threats.

Major Threat Actors

The Saudi government is a major target for cyberattacks. Specifically, state-owned oil producers, a sector of critical infrastructure, are at high risk. Since the attack against oil-producer Aramco, the Saudi government has been on high alert. Experts believe that the US's decision to pull out of the Iran nuclear

deal will increase cyberattacks from Iran (Perlroth, 2018). While there is a consensus that the Iranian government initiates cyberattacks, experts are not confident that the Iranian government conducted the 2012 Shamoon attack against Aramco (Zetter, 2015). An Iranian hacktivist group, known as Cutting Sword of Justice, is taking credit for the Aramco attack (Zetter, 2015). In addition to the attack against Aramco, there is evidence that this group is also responsible for several attacks on petrochemical plants in Saudi Arabia (Perlroth, 2018). An additional key actor in Saudi Arabia's cybersecurity strategy is a company called Hacker Team. Hacker Team sells hacking and surveillance technology exclusively to governments, and sells particularly well in authoritarian regimes (Franceschi-Bicchierai, 2018).

Pattern of Attacks

An overview patterns of attacks against Saudi Arabia allows for a comprehensive understanding of Saudi Arabia's place in the Middle East. In August of 2012, the world's largest oil producer company, Aramco, was attacked by a malware that is now known as Shamoon (Aleyani and Kumar, 2018). Cybersecurity experts are confident that the Iranian government holds some responsibility for the cyberattack against Saudi Arabia's state owned Aramco. Shamoon wiped data from 30,000 machines, and Aramco took almost two weeks to recover. Experts believe that the Iranian hackers used the same tactics used in Stuxnet.

While Shamoon gained international attention, a lesser known attack against Saudi Arabia that is still occurring in the country is Shamoon 2.0. Unlike Shamoon, this attack is not a single attack, but rather it is occurring constantly (Aleyani and Kumar, 2018). Generally, the attacks take place on weekends or holidays to give the malware time to infect more machines. Shamoon 2.0 shares 90% of the same code as Shamoon, but there are a few key differences. One difference between the two malwares is Shamoon 2.0 does not have a command and control communication, so the malware does not need to communicate back to the hackers. Additionally, Shamoon 2.0 features a ransomware module, which allows the hackers to further exploit victims. The victims are generally government entities in critical sectors in Saudi Arabia. Due to the increase in sophistication in the Shamoon 2.0 attack, the Iranian government may play a more significant role in these attacks (Aleyani and Kumar, 2018). The main motivation behind the attacks against Saudi Arabia is to gain political influence in the region and among Islamic States. Most of the attacks are wipers that are aimed at critical infrastructure.

National Cybersecurity Strategy

A discussion and analysis of Saudi Arabia's policy landscape, offensive cybersecurity strategy, tech industry collaboration, and education assesses both the strengths and weaknesses of Saudi Arabia's cybersecurity infrastructure and preparedness.

Offensive Cybersecurity Strategy

While Saudi Arabia does experience frequent cyberattacks, cybersecurity experts argue that Saudi Arabia, along with the UAE, is behind an attack against Qatar News Agency (Al Jazeera News, 2018). On May 24, 2017, state-owned news agency, Qatar News Agency, uploaded videos and quotes of the country's emir glorifying Islamic groups, such as Hamas and Iran (Pinnell, 2018). This created an immediate backlash from a total of nine governments, including Saudi Arabia, the UAE, and Egypt (Pinnell, 2018). Governments expelled Qatari citizens, suspended diplomats, and halted all trade (Pinnell, 2018). Saudi Arabia led the social media campaign accusing Qatar of funding radical Islamic groups. According to the Qatar Institute of Computerization, Saudi Arabia and the UAE created about 187 new Twitter accounts during and before the release of the fake news (Al Jazeera News, 2018). Saudi Arabia's crowned prince, Mohammed bin Salman, created a list of 13 demands for Qatar to meet within ten days (Pinnell, 2018). Some of the demands included shutting down Al Jazeera and removing all ties with Iran (Pinnell, 2018). The primary purpose for Saudi Arabia's offensive attacks is also political. However, instead of relying on only malware to attack other states in the region, Saudi Arabia uses a mixture of malwares and other advanced technology, developed and sold by the Hacker Team.

Policy Landscape

Due to the increase of cyberattacks against Saudi Arabia, the country has created government agencies to address threats to both the private and public sectors. In 2017, the National Cyber Security Center (NCSC) was created (Shamseddine, 2017). The NCSC provides defense systems, monitors threats, and responds to cyberattacks against critical infrastructure in Saudi Arabia. Their main goals include improving responses to cyberattacks and further developing internal capabilities in defending against cyberattacks (National Cyber Security Center, 2017). In 2018, the NCSC created a set of cybersecurity standards that must be applied to various state agencies (Taher, 2019).

Another agency in Saudi Arabia that addresses cybersecurity is the Communication and Information Technology Commission (CITC), which was created in 2001 (The Communications and Information Technology Commission, 2019). CITC has a wide range of responsibilities including information security awareness, protecting users' rights, and regulating domain name space in Saudi Arabia. The CITC works with both the public and private sectors (The Communications and Information Technology Commission, 2019).

Prince Salman has created and is working towards Saudi Arabia's Vision 2030 (Taher, 2019). One of the initiative's specific goals is positioning Saudi Arabia as an international, digital economic leader. The government plans to achieve this goal by investing and improving cybersecurity infrastructure, and

by creating the National Cybersecurity Authority. This agency is a national body that is focused on protecting, preventing, and deterring cyberattacks against the government. The leadership includes the head of state security, head of intelligence, and deputy interior minister (Taher, 2019).

In 2007, the Kingdom of Saudi Arabia released the Anti-Cyber Crime Law document (Bureau of Experts at the Council of Ministers, 2007). The document outlines which cybercrimes are considered to be against domestic law, and what the degree of punishment is for breaking the law (Bureau of Experts at the Council of Ministers, 2007). While the Saudi government argues that these laws are in place to protect their citizens and the country's sovereignty, many human rights experts argue that the government is excessively using the document to discourage online conversations critical of the government (Amnesty International, 2018).

Tech Industry Collaboration

Technology companies show a willingness to collaborate and meet the strict censorship demands of Saudi Arabia (Manjoo, 2017). The country's Vision 2030 specifically calls upon Saudi Arabia to diversify their economy. In achieving this goal, Saudi Arabia is investing billions in foreign tech companies (Manjoo, 2017). Saudi Arabia is the largest single investor in US tech startups, (Bensinger and Brown, 2018) and a large stakeholder in companies such as Apple, Twitter, and Snapchat (Manjoo, 2017). Uber alone has generated over $3.5 billion from the Saudi government (Manjoo, 2017). Saudi Arabia's willingness to heavily invest in tech companies provides the country with leverage when demanding that a company comply to the government's requests. Companies, such as Netflix, are willing to remove content and create censorship when the Saudi government requests (Dreyfuss, 2019).

A specific example of Saudi Arabia using investments to control collaboration between the country and companies is Saudi Arabia's relationship with Hacker Team. The director of the company is Adbullah Al-Qahtani, a prominent attorney, who primarily focuses on facilitating deals between the Saudi government and international organizations. The reason why a Saudi investor, and by proxy the Saudi government, might be interested in Hacker team's technology, is due to geopolitics in the region and the government's interest in surveillance among citizens. With an increase in cyberattacks against Saudi Arabia, the government is able to further justify increased internet surveillance on their citizens (Franceschi-Bicchierai, 2018).

Education

While Saudi Arabia is rapidly increasing investment in the tech industry to bring tech jobs to the country, Saudi Arabia lacks a workforce with the appropriate skills and education (Bensinger and Brown, 2018). The country has the Saudi Federation for Cyber Security and Programing, which focuses on

enhancing the Saudi population's cyberskills. The entity uses a wide range of techniques to achieve this goal, including organizing nationwide competitions that focus on coding, establishing partnerships with international cybersecurity firms, and creating more domestic college programs that teach cybersecurity (Al Arabiya, 2018). To meet Saudi Arabia's Vision 2030 initiative, the Saudi Federation for Cyber Security and Programing established a partnership with Booz Allen Hamilton (Al Arabiya, 2018).

International Internet Governance

In the new era of cyberwarfare and cybercrime, Saudi Arabia has become a target of cyberattacks. Saudi Arabia supports international internet governance and collaboration to create international cybersecurity norms that mitigate cyberattacks against governments.

Country Orientation

On international agreements, Saudi Arabia typically votes with Russia and China; yet unlike China and Russia, Saudi Arabia has no bilateral agreements. Along with other major actors such as the US, Russia, and China, Saudi Arabia has not agreed to the recent Paris Call (Uchill, 2018). The primary reason why Saudi Arabia has not signed on to the Paris Call for Trust and Security in Cyberspace is most likely because of the agreement's call for protection of citizens and focus on multi-stakeholder governance (Laudrain, 2018). Saudi Arabia is one of the 152 countries that signed onto the International Multilateral Partnership Against Cyber Threats (IMPACT) (Uchill, 2018). IMPACT is the first UN-backed cybersecurity alliance. The alliance provides countries with resources and expertise to better protect against cyberthreats. While Saudi Arabia is hesitant to work with private companies to create international internet agreements, the country is willing to cooperate with other governments.

Behavior at International Meetings

In general, Saudi Arabia tends to stay relatively quiet during international cybersecurity conferences. In recent debates held by the UN, including the General Assembly's conference in October of 2018, Saudi Arabia has not sponsored resolutions (United Nations, 2018). Saudi Arabia's contributions to International Telecommunication meeting resolutions tend to be minimal, but often include an emphasis on multilateral agreements. During international debates, Saudi Arabia typically focuses on the use of cyberweapons – especially Iran's constant attack on Saudi critical infrastructure (United Nations, 2016)

US-Saudi Arabia Alignment

The US and Saudi Arabia are strong allies who share common goals in the cybersphere. Both the US and Saudi Arabia agree that private companies need to create a backdoor on devices to allow governments to gain access (Kopfstein, 2015). Both countries also currently seek hacking help from the Hacker Team (Kopfstein, 2015). In 2015, the then NSA director Mike Rogers publicly argued for the

necessity of governments having access to encrypted data, or requiring that companies create a "backdoor" for the government (McCarthy, 2015). While there is room for cooperation between the US and Saudi Arabia, there are also barriers that could prevent a potential agreement occurring between the countries such as the US's strong free speech laws. Saudi Arabia requires all foreign information on the internet to be passed via one of three centralized access points, to sort out any information that is deemed as inappropriate. In 2018, Saudi officials announced their plans for prosecuting individuals who mock or disrupt the country's religious values (Blanchard, 2018 p16).

Shaping International Norms

Agreeing with most governments, Saudi Arabia encourages governments to work together to improve infrastructure and security in countries. This case demonstrates that Saudi Arabia understands the growing threat of cyberattacks, and that governments are vulnerable to manipulation from any international location. Any nation-state's corporations, infrastructure, and individuals are at risk of these threats, and Saudi Arabia agrees that international conversation, collaboration, and norms would strengthen international cybersecurity. Given its growing policy landscape, tech industry collaboration, and strong emphasis on education initiatives, Saudi Arabia will likely advocate for capacity-building when forming international cybersecurity norms. Saudi Arabia's alignment with the Budapest Convention, along with its public outcry against cyberterrorism, indicates both cybercriminal prosecution support and international cybersecurity policy cooperation between governments.

Victim State: Ukraine

By Eleanor Krabill

Table 17: Summary Findings, Ukraine

Major Attacks	
Attributed Threat Actor	**Actor Intent and Actions**
APT 28	Ukrainian power grids in Kiev and Ivano Frankivsk region disabled
GRU	Government attack on Ukrainian Finance Ministry, National Bank and State Treasury using ransomware
CyberBerkut	Election manipulation
Prolific Threat Actors	
Russian and pro-Russian cybercrime Ukrainian Hacktivists acting in defense of Ukraine or attacking Ukrainian government agencies for improvement	
Defensive Landscape	
Policies, Pending, and Passed	**Protections Provided**
Cyber Security Strategy of Ukraine	Conditions for the safe functioning of cyberspace for both private individuals and the public sector
The Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine	Legal definition of cybercrime, outlines state agencies and their obligations in provision of cybersecurity
Government Institutions	**Notable Publications**
State Service for Special Communications and Information Security	N/A
Ministry of Defense and General Staff of the Armed Forces of Ukraine	N/A
Intelligence Agencies of Ukraine	N/A
National Police of Ukraine	N/A
National Security and Defense Council	N/A
Security Service of Ukraine	N/A
International Orientation	
Multi/Bilateral Agreements	**Primary Goals**
Budapest Convention - Signatory	Pursue a common criminal policy aimed at the protection of society against cybercrime

Introduction

Ukraine's orientation towards creating international cybersecurity norms can be assessed by reviewing its profile of major adversaries and cyberattacks, weak and developing cybersecurity policy landscape, and behavior at international meetings. Ukraine's unique position as victim to Russian state aggression could be particularly helpful in shaping international cybersecurity norms. In addition to its political background, its cybersecurity policy landscape and international internet governance perspective implies that, given aid, support, and reservations to insulate it from further Russian attack,

the country will cooperate in the creation of future international cybersecurity norms. Table 17 summarizes the findings of this case study.

Background

In approaching Ukrainian cybersecurity, it is essential to address its complicated history and geopolitical position, which have uniquely motivated political cyberattacks on the young state. With more than half of its population connected to the internet, both Ukraine's history and ICT levels keep the nation continually vulnerable to cyberattacks.

Sociopolitical Vulnerabilities

Modern Ukraine is a nation in turmoil, under siege by Russia. Modern Ukraine did not exist as an independent state until 1991 after centuries of Russian domination (O'Hanlon, 2017). Ukraine's national identity centers on Ukrainian language and ethnicity, but a large and assertive Russian minority concentrated in the East undermines this identity. As a young nation, Ukraine has untried and weak institutions, low trust, and little respect for the rule of law (Chang, 2016; Vancraen, 2015; Zlenko, 2016). Following historical alliances has made Ukraine an internally divided nation in this quest for stability, with Eastern Ukraine and Crimea in support of Russia, and Western Ukraine in favor of EU and NATO membership. This deep division, running across historical lines of occupation, religious affiliations and, in some places, language barriers, has left the young nation susceptible to radical separatist movements and Russian interference (O'Hanlon, 2017). The lack of cohesion and immature security policy continues to leave Ukraine vulnerable to cyberattack.

Level of Connectivity

In the face of this deep political vulnerability to Russia and an underdeveloped cybersecurity regime, Ukranine's government and population are left exposed to cyberthreats. A majority of the Ukrainian population is connected to the internet, with 62% of households owning a computer, 58% with internet access at home and an estimated 25,129,261 internet users in the country (ITU- Ukraine, 2018). While this level of internet saturation is not among the highest internationally, it does represent a significant vector through which adversarial nation-states could influence and exploit the preexisting sociopolitical and cybersecurity issues present in Ukraine.

Major Threat Actors

As a result of Ukraine's tense relations with both the Russian government and Russian-sympathizing separatists at home, a majority of attacks sustained by Ukraine can be drawn back to one central actor, one central motivator: the Russian Federation.

Russia has launched the majority of the most devastating cyberattacks against Ukrainian businesses, government agencies, and infrastructure. In particular, the Central Directorate of Russian

intelligence, GRU, has taken a leading role in the Russo-Ukrainian conflict, both perpetrating attacks itself and by sponsoring APTs (Troianovski & Nakashima, 2018; FireEye, 2017). Russian partisan hacktivist organizations like CyberBerkut have also attacked the Ukrainian government, most notably interfering in the 2014 presidential election. Alongside other prominent hacktivists, CyberBerkut has also engaged in smaller scale hacks exposing sensitive Ukrainian government materials (Greenberg, 2017a ; Greenberg, 2017 b).

The Ukrainian government does not engage in offensive cyberattacks, although its present policies indicate an intention to do so in the future (as implied by the Ministry of Defense's assignment to respond to military aggression in cyberspace) (Poroshenko, 2016). Instead, Ukraine has depended on pro-Ukrainian hacktivists like CYBERHUNTA and RUH8 to gain sensitive materials, proving Russian involvement in 6,500 cyberattacks in the last two months of 2016 (Maurer, 2015; Zinets, 2016). Interestingly, other pro-Ukrainian hacktivists have hacked secure Ukrainian government servers in part to drive improvement of the Ukrainian cybersecurity system (Koval, 2015; Maurer, 2015).

Pattern of Attacks

Since 2014, Ukraine's government has been attacked in three major instances: the NotPetya attacks of 2017, the Power Grid Hacks of 2015 and 2016, and the 2014 election hacks. Each of these incidents posed a different threat both to Ukraine and to the international community as a whole, warranting attention and global concern and providing both Ukraine and its foreign counterparts incentives to collaborate in the development of future cybersecurity policy.

In perhaps the most publicized of the attacks Ukraine has been subjected to in the last five years, GRU-linked APT-28 hackers shut down Ukraine's power grid, displaying the vulnerability of international critical infrastructure to Russia. Using complex BlackEnergy3 and Industroyer trojan malware, Russian hackers were able to perform a synchronized attack on the power grid and the telecommunications network, leaving 230,000 Ukrainians without power or phone service for six hours in 2015 and again in 2016 (Greenberg, 2017a; Greenberg, 2017b).

In 2014, CyberBerkut launched a multi-tiered attack on the Ukrainian presidential election. CyberBerkut engaged in a hack and disinformation campaign against the Ukrainian Central Elections Commission that undermined confidence in the election and sowed confusion and distrust among the Ukrainian voter base (Koval, 2015; Streltsov, 2017). As determined by the former head of CERT-UA and considering the complexity of this attack, it is highly probable that CyberBerkut carried out these attacks in conjunction with Russian state actors (Koval, 2015).

In 2016, the GRU attacked the Ukrainian National Bank, Finance Ministry, and State Treasury with wiper malware, masquerading as ransomware (Fulton Beale, 2018). The NotPetya malware demanded $300 in bitcoin from infected computers to restore critical files, while instead permanently deleting them (Streltsov, 2017). The NotPetya malware spread rapidly, costing the Ukrainian government an estimated $500 million dollars and the international economy an estimated $10 billion (Fulton Beale, 2018). As a result of this attack, pensioners missed retirement benefits, and public trust in the Ukrainian government fell sharply (Greenberg 2017c).

What these attacks all have in common is that they are all politically motivated, intended to weaken Ukraine relative to Russia; they seek to undermine the Ukrainian state, Ukrainian institutions, and public trust. This can largely be inferred from the targets and timing of the three aforementioned attacks. The Ukrainian power grid hacks have been linked to the Ukrainian Rada's decision to nationalize power companies with ties to Russian oligarchs close to Putin (Zetter, 2015). The election hacks of 2014 compromised Ukraine's first election after the ouster of pro-Russian Viktor Yanukovych and concurrently with the Russian annexation of Crimea, and the NotPetya attacks not only specifically targeted Ukrainian state ministries, but the attack was launched on Ukrainian independence day. All three of these noteworthy attacks launched by Russian state organizations and pro-Russian actors were, therefore, launched to defend Russian interests and spite the Ukrainian government.

These attacks, too, have raised international concern because of their political nature and the broad implications of these kinds of attacks in their Russian origin. Indeed, it appears that through these attacks, not only has Russia been testing its capabilities, but has been testing what offenses are internationally acceptable (Greenberg, 2017b). After these attacks on Ukraine received little international backlash, BlackEnergy malware was found on US power utilities servers, Russia attempted similar meddling in the French, German and American Elections, and the NotPetya virus wreaked havoc internationally (Greenberg, 2017b). Thus, for the international community, the attacks sustained by Ukraine are indicative of possible attacks on their own infrastructure in the future, should they come into conflict with Russian ideals.

National Cybersecurity Strategy

Ukraine's cybersecurity strategy remains underdeveloped, as can be seen through a discussion and analysis of its policy landscape, tech industry collaboration, and education programs. The lack of maturity, inter-agency agency communication, and extra governmental coordination displayed in Ukrainian cybersecurity has led Ukraine to accept help from the international community and to participate in international internet governance discussions.

Policy Landscape

As a result of its geopolitical situation, Ukraine's cybersecurity regime is largely defensive, reactionary, and contingent. Prior to 2014, Ukraine did not have a cybersecurity strategy and it did not invest in cyberdefense (Streltsov, 2017). After recent damaging attacks, Ukraine has recognized the need for cohesive cybersecurity policy. Since 2014, Ukraine has promulgated the Cyber Security Strategy of Ukraine and the 2017 Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine. These policies highlight the desire to build Ukraine's cyberdefense capabilities ("…Basic Principles Ensuring Cyber, 2017…"). While outlining the need for improved cybersecurity, public education, and international cooperation in the maintenance of a safe internet, these policies remain underdeveloped.

These laws, recognizing the necessity of a multifaceted system of cyberdefense, created six cyberdefense agencies under the departments of the Security Service, the Ministry of Defense, the National Police, the National Security and Defense Council, the State Service for Special Communications and Information Security, and the National Bank ("…Basic Principles Ensuring Cyber, 2017…"). Under the law of Basic Principles Ensuring the Cyber Security Yet, because they lack central coordination, these institutions cannot effectively combat cybercrime (Kostyuk, 2018).

Tech Industry Collaboration

The official cybersecurity policies of 2015 and 2017 call for public-private cooperation in cybersecurity research and public education (Poroshenko, 2016; Basic Principles Ensuring Cyber, 2017). However, with no legal framework or cybersecurity research institutions, public-private partnerships have not developed. As a result, Ukraine's private sector has operated independently with limited resources (Streltsov, 2017).

Education

Despite the prominence of public education in official cybersecurity strategy, the Ukrainian government has taken no action to implement media literacy or cybersecurity education policies. Instead, private citizens and organizations have been providing such training. International organizations such as Internews and IREX (International Research and Exchange Board) have hosted media literacy youth summer camps and Learn to Discern training to give the public tools to recognize and resist disinformation campaigns (Susman-Peña and Vogt, 2017; Guthrie, 2018). The Ukrainian news media, too, has worked to inform the general public about disinformation campaigns and debunk prominent and widely circulated "fake news" through projects like StopFake.org (Shankovskiy). While government aid would help, these private actions continue to improve Ukrainian cybersecurity.

International Internet Governance

As a constant victim of cyberattacks, Ukraine has chosen to pursue the creation of multi-stakeholder international cybersecurity norms to enhance its security in the present and in the future; it does so, however, with reservations to preserve its sovereignty and insulate itself from the Russian federation. These conflicting intentions can be inferred from their ratification of the Budapest convention, acceptance of international aid for capacity building, and rejection of the Paris Call. This security-driven, reserved embrace of international internet governance has led Ukraine to cooperate in IGF and other international internet governance fora as an enthusiastic and active participant.

Country Orientation

The Ukrainian government officially supports international internet governance. In every national cybersecurity strategy document, Ukraine emphasizes the importance of a universal, open and innovative internet (National Cybersecurity Strategy). Ukraine has worked for years to align its cybersecurity policy with the EU, NATO, and the Council of Europe. To that end, Ukraine has signed all three Council of Europe cybercrime conventions. Both NATO and EU have provided aid and expertise to strengthen Ukraine's fledgling cybersecurity regime (TAIEX Expert Mission…, 2018; Treaty 201, 2007; Treaty 210,2011; Budapest Convention, 1994; Enhancing Cyber Security in Ukraine, 2018).

In contrast, Ukraine has engaged in state-level censorship campaigns in the last several years for national security reasons. Fearful of further Russian incursion and the pariah state's continuing influence over Ukraine, President Poroshenko restricted access to several popular Russian social media platforms, email servers and search engines. Indeed, Ukraine would like to comply fully with international standards of internet governance, but it is precisely this international nature that leaves Ukraine exposed to Russian threats; a truly international, multi-stakeholder internet would leave room for Russian disinformation and further incursion on the Ukrainian government's sovereignty. Thus Ukraine's position on international internet governance can be understood, through observation of its censorship activities, as one of reserved enthusiasm. Ukraine highly values the idea of an international multi-stakeholder system of governance, but, for security reasons, preferring one that allows for some degree of national internet sovereignty.

Behavior at International Meetings

In keeping with its official stance on internet governance, Ukrainian representatives have consistently attended the international Internet Governance Forum since 2007, contributing to the international dialogue, voicing Ukrainian concerns and hosting round table discussions (IGF attendance reports 2007-2018). Ukraine has engaged in several regional internet governance forums, as well as IGF and IGF UA, to foster international and multi-stakeholder analysis and discussion of Eastern European

and Ukrainian Internet Governance in particular (SEEDIG, 2018; IGF UA, 2018). These actions, in conjunction with Ukraine's continuing efforts to align itself with international cybersecurity standards, indicate consistent support of cooperative international multi-stakeholder internet governance.

US-Ukraine Alignment

Ukraine and the US are established partners in the cyberrealm, promoting the establishment and improvement of each other's defenses, and voting similarly in international cybersecurity meetings. Both nations recognize Russia as a primary cyberadversary.

Over the last two years, as a result of the new US-Ukraine Cybersecurity Dialogues, Ukraine and the US have pursued projects together to strengthen cybersecurity incident response capacity, awareness, and trainings within agencies ("Second U.S.-Ukraine…", 2018). Doing so allows the US to monitor Russian tactics and test its own defenses, while also helping an ally. To that end, the US gave $10 million to improve Ukrainian cybersecurity in 2018 (Lyngaas, 2018). Additionally, the US and Ukraine both rejected the 2018 Paris Call due to concerns that signing such an agreement would prevent both nations from building deterrent or retaliatory cyberweapons of their own, and would specifically prevent Ukraine from any internet censorship (Liste des Soutiens à l'appel de Paris, 2018). Such voting patterns indicate a shared political outlook that predisposes both countries to act as an international internet governance unit.

Ukraine's partnership with the US, however, is a guarded one. As a fledgling state in 1994, Ukraine ceded its main source of defense against the Russian Federation (Budapest Memorandum, 1994). Ukraine embraced the "security assurances" of the United States and the United Kingdom as granted in the Budapest Memorandum, in exchange for its nuclear weapons (Budapest Memorandum, 1994). Over the next 20 years, Ukraine invested little in its armed forces relying on that security guarantee. In 2014, when Russia annexed Crimea, the US did not respond militarily. Ukraine then lost confidence in its strategic partnership with the US, and to-date remains wary of future US alliances.

Shaping International Norms

Ukraine prefers a multi-stakeholder approach to the creation of international cybersecurity norms as it allows the young, developing, democracy's cybersecurity competency to grow with the protection and aid of the wider international community. As this case demonstrates, Ukraine is acutely aware of the growing threat that cyberattacks pose to critical infrastructure, information security, and finances which, under their current cybersecurity regime, are left vulnerable to manipulation and corruption by outside forces. For this reason, Ukraine has a vested interest in improving not only its own cybersecurity, but fostering a dialogue that allows for international cooperation in the establishment of

norms to strengthen global cybersecurity. However, as primarily a victim of cyberattack, Ukraine stands in a unique position, needing to defend itself against its formidable Russian adversary in any and all ways. Ukraine, therefore, would favor the creation of multi-stakeholder international cybersecurity policies that would allow its interests as a victim state and its security to be addressed.

Thus, in establishing future cybersecurity policy, Ukraine is likely to heavily favor a treaty following the NPT model, proposed by a neutral state, addressing both victim and aggressor states, providing incentives to nonaggressive states and victim states alike in the form of capacity building and working towards the establishment of international cybersecurity norms while providing a national security escape clause. This model, for Ukraine and for other victim states, would provide the international security framework necessary to accept an international cybersecurity agreement without reservation.

Bibliography

"超级火焰"病毒已入侵我国 ["Flame" Has Invaded China] (2012, July 2). Retrieved from http://netsecurity.51cto.com/art/201207/345474.htm

18F: Digital service delivery | About. (n.d.). Retrieved March 1, 2019, from https://18f.gsa.gov/about/

About - National Initiative for Cybersecurity Education (NICE). (2017, January 20). Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/about

About us - NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). Retrieved from https://ccdcoe.org/about-us/.

Advanced Persistent Threat Groups: Who's who of cyber threat actors. (n.d.) *FireEye.* Retrieved from https://www.fireeye.com/current-threats/apt-groups.html

Advanced Persistent Threat Groups. (2019). *FireEye*. Retrieved from

African Union (AU) Cyber Security Expert Group. (2018). *African Union Cyber Security Expert Group Terms of Reference*. Retrieved from https://au.int/sites/default/files/announcements/34877-annc-au_cyber_security_expertgroup_tors.pdf

African Union Headquarters. (2014, June 27). *African Union Convention on Cyber Security and Personal Data Protection.* Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Ahmad, I. & Culum, P. (2017, April 7). Cyber Security Risk Management in Canada: Nine Things Happening in 2017. Fire Eye Blog. Retrieved from https://www.fireeye.com/blog/executive-perspective/2017/04/cyber_security_risk.html

Al-Arabiya Staff Writer. (2018, March 21). Saudi Arabia signs Cyber Security MoU with Booz Allen Hamilton. *Al-Arabiya.* Retrieved from http://english.alarabiya.net/en/business/economy/2018/03/21/Saudi-Arabia-signs-Cyber-Security-MoU-with-US-company.html

Albert, E. (2015). The Shanghai Cooperation Organization Backgrounder. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/backgrounder/shanghai-cooperation-organization

Albert, E. (2018, March 28). Understanding the China-North Korea Relationship. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/backgrounder/china-north-korea-relationship

Alelyani, S., & Kumar, H. (2018). Overview of Cyberattack on Saudi Organizations. *Journal of Information Security and Cybercrimes Research,* 1(1). Retrieved from https://journals.nauss.edu.sa/index.php/JISCR

Allen-Ebrahimian, B. (2017, June 20). 64 Years Later, CIA Finally Releases Details of Iranian Coup. *Foreign Policy.* Retrieved February 20, 2019, from https://foreignpolicy.com/2017/06/20/64-years-later-cia-finally-releases-details-of-iranian-coup-iran-tehran-oil/

Ambrosio, T. (2008). Catching the 'Shanghai Spirit': How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia. *Europe Asia Studies,* 60(8), (pp. 1321-1344). Retrieved from https://www.jstor.org/stable/20451609

Amnesty International. (n.d.). *Saudi Arabia 2017/2018*. Retrieved from https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/report-saudi-arabia/

Andersen, L. R. (2018, November 16). The Paris Peace Forum—What's Not to Like? [News]. Retrieved from https://theglobalobservatory.org/2018/11/paris-peace-forum-whats-not-to-like/

Armerding, T. (2017, January 31). Obama's cybersecurity legacy: Good intentions, good efforts, limited results. Retrieved from https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html

Armstrong, C. (2013). *Tyranny of the Weak: North Korea and the World, 1950-1992*. Cornell Press.

Baezner, M. (2018, August). Regional rivalry between India-Pakistan: tit-for-tat in cyberspace. *CSS Cyber Defense Project*. Retrieved from https://www.researchgate.net/publication/326866504_Regional_rivalry_between_India-Pakistan_tit-for-tat_in_cyberspace

Baker, C. (2019, January 16). Canada is a prime target for cybersecurity attacks in 2019. *IT World Canada.* Retrieved from https://www.itworldcanada.com/article/canada-is-a-prime-target-for-cybersecurity-attacks-in-2019/414201

Bannelier-Christakis, K. (2015). Chapter 16: Is the principle of distinction still relevant in cyberwarfare? In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 343–365). Edward Elgar Publishing. Retrieved from https://www-elgaronline-com.offcampus.lib.washington.edu/view/9781782547389.00028.xml

Barton, R. (2014, July 29). Chinese cyberattack hits Canada's National Research Council. *CBC News*. Retrieved from https://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

BBC News. (2019, February 18). *India country profile*. Retrieved from https://www.bbc.com/news/world-south-asia-12557384

Beale, N.F. (2018). Ukraine Has Become a Cybersecurity Front Line. Retrieved from https://theubj.com/news/view/ukraine-has-become-a- cybersecurity-front-line

Beaubien, J. (2018, April 2). The Country With The World's Worst Inequality Is... *National Public Radio.* Retrieved from https://www.npr.org/sections/goatsandsoda/2018/04/02/598864666/the-country-with-the-worlds-worst-inequality-is

Beefy, D. (2017, October 31). State-sponsored cyberattacks on Canada successful about once a week, *CBC News*. Retrieved from https://www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711

Belin, C. (2018, November 9). What the Paris Peace Forum tells us about France—and about the world. *Brookings Institute.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2018/11/09/what-the-paris-peace-forum-tells-us-about-france-and-about-the-world/

Belkin, P. (2018, April 19). France and U.S.-French Relations: In Brief. *Congressional Research Service*. Retrieved from https://fas.org/sgp/crs/row/R45167.pdf

Berger, R. (2018, April 10). Canada's Mandatory Privacy Breach Reporting Requirements coming into force November 1, 2018. Data Protection Report. Retrieved from https://www.dataprotectionreport.com/2018/04/canadas-mandatory-privacy-breach-reporting-requirements-coming-into-force-november-1-2018/

Beuth, P. (2016, January 29). Alles Wichtige zum NSA-Skandal. *Zeit Online.* Retrieved from https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal

Bienvenue sur Québec.ca. (n.d.). Retrieved from https://www.quebec.ca/

Bing, C. (2018, November 8). U.S. accuses China of violating bilateral anti-hacking deal. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E

Bing, C. & Lynch, S. (2018). U.S. Charges North Korean Hacker in Sony, WannaCry Cyberattacks. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-northkorea-sony-idUSKCN1LM20W

Blanchard, C. M. (2018, September 21). Saudi Arabia: Background and U.S. Relations. *Congressional Research Service*, 51. Retrieved from https://fas.org/sgp/crs/mideast/RL33533.pdf

Blogger, G. (2016, September 15). Shouting at Americans: A Peek Into French Signals Intelligence. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/shouting-americans-peek-french-signals-intelligence

Boyle, B. F. (2018). H.R.1997 - 115th Congress: Ukraine Cybersecurity Cooperation Act of 2017. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/1997/text

Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., … Dredze, M. (2018). Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate. *Am J Public Health,* 108(10), (pp. 1378-1384). Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6137759

Bronskill, J. (2018, December 20). Advanced Persistent Threat 10: Canada among targets of alleged Chinese hacking campaign. *National Post.* Retrieved from https://nationalpost.com/news/canada/canada-among-targets-of-alleged-chinese-hacking-campaign

Brown, E., & Bensinger, G. (2018, October 16). Saudi Money Flows Into Silicon Valley—and With It Qualms. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/saudi-backlash-threatens-u-s-startups-1539707574

Buchanan, B., & Sulmeyer, M. (2016). Russia and cyber operations: Challenges and opportunities for the next U.S. administration. *Carnegie Endowment for International Peace.* Retrieved from https://carnegieendowment.org/2016/12/13/russia-and-cyber-operations-challenges-and-opportunities-for-next-u.s.-administration-pub-66433

Bundesamt fuer Sicherheit und Informationstechik. (2015, July 17) Das IT-Sicherheitsgesetz. Retrieved from https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1550434030777

Bundesamt fuer Sicherheit und Informationstechnik. (2018, September). Die Lage der IT-Sicherheit in Deutschland. Retrieved from https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3

Burton, G. (2018, June 18). US Cyber Command given powers to launch cyber attacks on other nations. Retrieved from https://www.computing.co.uk/ctg/news/3034348/us-cyber-command-given-powers-to-launch-cyber-attacks-on-other-nations

Busby, M. (2018, September 6). North Korean 'hacker' Charged over Cyber-Attacks against NHS. *The Guardian*. Retrieved from https://www.theguardian.com/world/2018/sep/06/us-doj-north-korea-sony-hackers-chares

Calburn, T. (2009, November 20). China Cyber Espionage Threatens U.S., Report Says. *Dark Reading*. Retrieved from https://www.darkreading.com/risk-management/china-cyber-espionage-threatens-us-report-says/d/d-id/1085047

Campion-Smith, B. (2013, September 16). Discovery of Russian spy in Canadian navy set off sabotage fears. *The Star*. Retrieved from https://www.thestar.com/news/canada/2013/09/16/discover_of_spy_in_canadian_navy_set_off_sabotage_fears.html

Canadian Internet Registration Authority. (2016, December 2). *Internet use in Canada.* Retrieved from https://cira.ca/factbook/domain-industry-data-and-canadian-Internet-trends/internet-use-canada

Canadian Internet Registration Authority. (2018, October 10). *Fall 2018 Cyber Security Survey Report* [report]. Retrieved from https://cira.ca/2018-cybersecurity-survey-report

Canadian Security Intelligence Service Homepage. (2017, November 21). Retrieved from https://www.canada.ca/en/security-intelligence-service.html

Canadian Trade Commissioner Service (2018, June 20). *Canada's Innovation Strengths and Priorities.* Retrieved from http://www.tradecommissioner.gc.ca/innovators-innovateurs/strategies.aspx?lang=eng

Carnegie Endowment for International Peace. (2019). *Cyber Norms Index.* Retrieved from https://carnegieendowment.org/publications/interactive/cybernorms

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), (pp. 43–62). Retrieved from https://doi.org/10.1111/1468-2346.12504

Center for Strategic & International Studies. (n.d.). *Significant Cyber Incidents Since 2006.* Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/190103_Significant_Cyber_Events_List.pdf

Center for Strategic and International Studies. (2014). *Significant Cyber Incidents Since 2006* (pp. 15). Brown University. Retrieved from http://cs.brown.edu/courses/cs180/static/files/lectures/readings/lecture2/Cyber%20Incidents%20Since%202006.pdf

Center for Strategic and International Studies. (2017, May). *Significant Cyber Incidents Since 2006.* Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/170519_Significant_Cyber_Events_List.pdf?HJ4k1Bt7x.zleLsdr9m6SQbkWHtuNJ39

Centre for International Governance Innovation. (2018). *Governing Cyber Security in Canada, Australia and the United States Special Report* [report]. Retrieved from https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf

Chang, M. (n.d.). Corruption and Institutions in Ukraine, 44.

Chanlett-Avery, E., Rosen, L. W., Rollins, J. W., & Theohary, C. A. (2017, August 3). North Korean Cyber Capabilities: In Brief (pp. 13). *Congressional Research Service*.

Chappell, B., & Neuman, S. (2017, December 19). U.S. Says North Korea "Directly Responsible" For WannaCry Ransomware Attack. *National Public Radio.* Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Charlet, K. (2018). Understanding Federal Cybersecurity. *Belfer Center for Science and International Affairs*, 58.

Chen, A. (2015, June 2). The agency. *The New York Times.*

Chernenko, E., Demidov, O. & Lkyanov, F. (2018, February 23). Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Chowdhry, A. (2016, March 28). U.S. and Germany Expand cyber cooperation. *Federal Computer Week.* Retrieved from https://fcw.com/articles/2016/03/28/us-germany-cyber.aspx

Cimpanu, C. (2010). Russian APT Comes Back to Life with New US Spear-Phishing Campaign. *ZDNet*. Retrieved from https://www.zdnet.com/article/russian-apt-comes-back-to-life-with-new-us-spear-phishing-campaign/

Clark, I. (2011). China and the United States: A succession of hegemonies? *International Affairs (Royal Institute of International Affairs)*, 87(1) (pp. 13-28). Retrieved from http://www.jstor.org/stable/20869608

Clough, J. (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*, 40(3). Retrieved from https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf

Cobb, Stephen. (2018, November 18). Cybersecurity a big concern in Canada as cybercrime's impact grows. Retrieved from https://www.welivesecurity.com/2018/11/19/cybersecurity-big-concern-canada-cybercrime/

Communication and Information Technology. (2019). *Roles and Responsibilities.* Retrieved from http://www.citc.gov.sa/en/aboutus/areasofwork/Pages/default.aspx

Communications Security Establishment. (2011, October 31). Mission, Vision and Values. Retrieved from https://www.cse-cst.gc.ca/en/about-apropos/vision-mission

Communications Security Establishment. (2018, June 11). Canadian Centre for Cyber Security: Overview. Retrieved from https://www.cse-cst.gc.ca/en/backgrounder-fiche-information

Constantin, L. (2015, March 9). Cyberespionage arsenal could be tied to French intelligence. *IT News*. Retrieved from https://www.computerworld.com/article/2894379/cyberespionage-arsenal-could-be-tied-to-french-intelligence.html

Constitution of the Islamic Republic of Iran. (1989). Government of Iran.

Corera, G. (2016, October 10). How France's TV5 was almost destroyed by "Russian hackers". *BBC News* Retrieved from https://www.bbc.com/news/technology-37590375

Corfield, G. (2019, January 22). En garde! "Cyber-war has begun" – and France will hack first, its defence sec declares. *The Register*. Retrieved from https://www.theregister.co.uk/2019/01/22/france_cyber_war/

Council of Europe - Budapest Convention and related standards. (n.d.). Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (2007, October 25). *Details of Treaty No. 201.* Treaty Office. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201

Council of Europe. (2011, November 5). Complete list of the Council of Europe's treaties. Retrieved February 7, 2019 from https://www.coe.int/en/web/conventions/full-list

Council of Europe. (2018). *Budapest Convention and related standards.* Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Council of Europe. (2019, February 6). *Complete list of the Council of Europe's treaties*. Retrieved from https://www.coe.int/en/web/conventions/full-list

Council of Europe. (2019). *Chart of signatures and ratifications of Treaty 185.* Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Council of Europe. (n.d.). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY* [chart]. Retrieved from https://www.coe.int/en/web/cybercrime/parties-observers

Crowdstrike Global Intelligence Team. (2016, December 22). *Use of Fancy Bear Android malware in the tracking of Ukrainian field artillery units.* Retrieved from https://freewhitewater.com/wp-content/uploads/2016/12/FancyBearTracksUkrainianArtillery.pdf

Cyber attack on France targeted Paris G20 Files. (2011, March 7). *BBC News.* Retrieved from https://www.bbc.com/news/business-12662596

Cyber Policy Institute. (2017). *Membership of the UN Group of Government Experts (UN GGE) 2004-2017.* Retrieved from https://ict4peace.org/wp-content/uploads/2017/02/CPI-UN-GGE-Members-2004-2017.pdf

Cyber Security Agency of Singapore. (2018, November 16). Singapore and the United States sign Declaration of Intent on Cybersecurity Technical Assistance Programme. Government of Singapore. Retrieved from http://www.csa.gov.sg/news/press-releases/singapore-and-the-us-sign-doi-on-cybersecurity-technical-assistance-programme

Cyberattack during the Paris G20 Summit. (2017, August 15). Retrieved from https://en.wikipedia.org/wiki/Cyberattack_during_the_Paris_G20_Summit

Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. (n.d.) Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 1(1), (pp. 24–34). Retrieved from https://pdfs.semanticscholar.org/174b/4bd588306e3fa0067eda83df61719a0996ce.pdf

Davidson, L. (2016, June 30). Despite Cyber Agreements, Russia and China Are Not as Close as You Think. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/despite-cyber-agreements-russia-and-china-are-not-close-you-think

Dehghan, S. K. (2012, January 5). Iran clamps down on internet use. The Guardian. Retrieved from https://www.theguardian.com/world/2012/jan/05/iran-clamps-down-internet-use

Delerue, F. & Géry, A. (2018, March 23). France's Cyberdefense Strategic Review and International Law. *Lawfare*. Retrieved from https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law

Denning, D. (2018, February 20). North Korea's growing criminal cyberthreat. *The Conversation.* Retrieved from http://theconversation.com/north-koreas-growing-criminal-cyberthreat-89423

Denning, S. (2018, December 19). How Russia Is Still Running Interference For Trump. *Forbes.* Retrieved from https://www.forbes.com/sites/stevedenning/2018/12/19/how-putin-augments-trumps-disinformation-against-the-russia-probe/

Department of Defense. (2018). *Cyber Strategy* (pp. 7). Government of the United States. Retrieved from https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Foreign Affairs and Trade. (2017, July 13). *Joint Statement from Australia-India Cyber Policy Dialogue* [statement]. Government of Australia. Retrieved from https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Bilateral/Australia-India+Cyber+Policy+Dialogue+7-13-2017.pdf

Department of Justice and Constitutional Development. (2017, June 27). Special Investigating Unit and PSETA signs MOU on cyber crime with French Embassy, 28 Jun [press release]. Government of South Africa. Retrieved from https://www.gov.za/xh/speeches/special-investigating-unit-and-pseta-signs-mou-cyber-crime-french-embassy-28-jun-27-jun

Dickson, J. (2018, June 5). Canada's 2019 election a likely target for Russian hackers, James Comey warns. *Global News Canada.* Retrieved from https://globalnews.ca/news/4255411/canadas-2019-election-russian-hacking-comey/

Dorigo, L. (2016, December 1). Inside Iran's "Silicon Valley." Aljazeera. Retrieved from https://www.aljazeera.com/indepth/inpictures/2016/11/iran-silicon-valley-161130094759722.html

Doughtery, K. (2018, October 9). Quebec nationalism key to Coalition's plan for power. *iPolitics*. Retrieved from https://ipolitics.ca/2018/10/09/quebec-nationalism-key-to-coalitions-plan-for-power/

Dowling, S. (2018, October 24). Startups Lock Down Government Contracts As Cybersecurity Concerns Grow. Retrieved from https://news.crunchbase.com/news/startups-lockdown-government-contracts-as-cybersecurity-concerns-grow/

Dreyfuss, E. (2019, January 4). Saudi Arabia Won't Be the Last Country to Censor Netflix. *Wired*. Retrieved from https://www.wired.com/story/saudi-arabia-netflix-censorship/

Ducheine, P. (2015). Chapter 10: The notion of cyber operations. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 211–232). Edward Elgar Publishing. Retrieved from https://www-elgaronline-com.offcampus.lib.washington.edu/view/9781782547389.00021.xml

Eilstrup-Sangiovanni, M. (2018). Why the World Needs an International Cyberwar Convention. *Springer Netherlands: Philosophy and Technology*, 31(3), (pp. 379–407). Retrieved from https://link.springer.com/article/10.1007/s13347-017-0271-5

Electoral Systems. (2018). *Ace Project.* Retrieved from http://aceproject.org/ace-en/topics/es/esd/esd02/esd02e/esd02e03

Internet Governance Forum. (n.d.). Electronic Frontier Foundation. Retrieved from https://www.eff.org/igf.

Emmott, R. (2018, October 16). NATO cyber command to be fully operational in 2023. *Reuters*. Retrieved from https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9

Ermert, M. (2018, November 12). IGF Needs Bold Reform, Internet Needs More Regulation, Says President Macron. *Intellectual Property Watch*. Retrieved from http://www.ip-watch.org/2018/11/12/igf-needs-bold-reform-internet-needs-regulation-says-president-macron/

Esch, C. (2018, October 19). The Rise of Russia's GRU Military Intelligence Service. *Der Spiegel.*

European Union. (2018, December 11). Cybersecurity Act. https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

Fazzini, K. (2019, January 16). Recorded Future research shows how Iranian hackers collaborated. CNBC. Retrieved from https://www.cnbc.com/2019/01/16/new-research-offers-a-glimpse-inside-the-online-forums-where-iranian-hackers-congregate.html

China responsible for over a third of cyber attacks on official Indian sites, NSCS informed. (2018, August 23). *Financial Express*. Retrieved from https://www.financialexpress.com/india-news/china-responsible-for-over-a-third-of-cyber-attacks-on-official-indian-sites-nscs-informed/1289272/

Federal Government and Private Sector to Collaborate through the Pipeline Cybersecurity Initiative. (2018, October 24). Retrieved from https://www.huntonprivacyblog.com/2018/10/24/federal-government-and-private-sector-to-collaborate-through-the-pipeline-cybersecurity-initiative/

Federal Information Security Modernization Act of 2014. (2014, December 18). Public Law 113-283, Sec. 3553(a)(1). Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

FireEye iSIGHT Intelligence. (2017, January 11). *APT28: At the Center of the Storm.* Retrieved from https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html

FISMA Background - Risk Management. (2016, November 30). Computer Security Resource Center, National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/projects/risk-management/detailed-overview

France hit by unprecedented wave of cyber attacks. (2015, January 15). *CBS News*. Retrieved from https://www.cbsnews.com/news/france-hit-by-19000-cyber-attacks-after-charlie-hebdo-terror-attacks/

France thwarts 24,000 cyber-attacks against defence targets. (2017, January 8). *BBC News.* Retrieved from https://www.bbc.com/news/world-europe-38546415

France's Renault hit in worldwide 'ransomware' cyber attack. (2017, May 12). *France 24.* Retrieved from https://www.france24.com/en/20170512-cyberattack-ransomware-renault-worldwide-british-hospitals

Franceschi-Bicchierai, L., Koebler, J., & Mead, D. (2018, January 31). Hacking Team Is Still Alive Thanks to a Mysterious Investor From Saudi Arabia. *VICE News.* Retrieved from https://motherboard.vice.com/en_us/article/8xvzyp/hacking-team-investor-saudi-arabia

Fraser, N., O'Leary, J., Cannon, V., & Plan, F. (2018, October 3). APT38: Details on New North Korean Regime-Backed Threat Group. *FireEye.* Retrieved from https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html

Full Text: International Strategy of Cooperation on Cyberspace. (2017, March 1). *Xinhua News Agency.* Retrieved from http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm

Fulton, Jonathan. (2018). Could the SCO Expand Into the Middle East? *The Diplomat*. https://thediplomat.com/2018/02/could-the-sco-expand-into-the-middle-east/.

Gady, F., & Austin, G. (2010). Russia, the United States, and cyber diplomacy. *EastWest Institute.* Retrieved from https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

Gallagher, S. (2015, June 30). Researchers expose Dino, espionage malware with a French connection. Retrieved from https://arstechnica.com/information-technology/2015/06/researchers-expose-dino-espionage-malware-with-a-french-connection/

Geers, K. (2011). *Strategic Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence.

Geers, K. (2015). *Cyber war in perspective: Russian aggression against Ukraine.* NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

Germany Develops Offensive Cyber Capabilities Without a Coherent Strategy of What to do With Them. (2018, December 3). *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them

Germany's Deep Cooperation with the NSA. (2014, June 18). *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html

Glenza, J. (2018, August 23). Russian trolls 'spreading discord' over vaccine safety online. *The Guardian.*

Goel, V. (2018, August 31). India Pushes Back Against Tech 'Colonization' by Internet Giants. *The New York Times.* Retrieved from https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html

Government of Canada, R. C. M. P. (2014, December 16). Cybercrime: an overview of incidents and issues in Canada | Royal Canadian Mounted Police. Retrieved from http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec3

Government of Canada, S. C. (2018, December 14). Impact of cybercrime on Canadian businesses, 2017. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm

Government of Canada. (2013). *Action plan 2010-2015 for Canada's cyber security strategy* [report]. Ottawa: Government of Canada. Retrieved from https://central.bac-lac.gc.ca/.item?id=PS9-1-2013-eng&op=pdf&app=Library

Government of Canada. (2015, July 8). Canada Completes Ratification of Convention on Cybercrime [news release]. Retrieved from https://www.canada.ca/en/news/archive/2015/07/canada-completes-ratification-convention-cybercrime.html

Government of Canada. (2015, June 18). Statement from Minister Blaney on today's cyber-attack [statement]. Retrieved from https://www.canada.ca/en/news/archive/2015/06/statement-minister-blaney-today-cyber-attack.html

Gowan, R. (2018, November 12). Peacemaking Is More Complicated Than Ever. The Paris Peace Forum Shows Why. *World Politics Review.* Retrieved from https://www.worldpoliticsreview.com/articles/26722/peacemaking-is-more-complicated-than-ever-the-paris-peace-forum-shows-why

Grassegger, H., & Krogerus, M. (2017, December 2). Fake news and botnets: How Russia weaponised the web. *The Guardian.*

GReAT. (2015, March 6). Animals in the APT Farm. Retrieved from https://securelist.com/animals-in-the-apt-farm/69114/

GReAT. (2017, April 3). Lazarus Under The Hood. Retrieved from https://securelist.com/lazarus-under-the-hood/77908/

Greenberg, A. (2017, May 9). The NSA Confirms It: Russia Hacked French Election "Infrastructure". *Wired*. Retrieved from https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/

Greenberg, A. (2017, June 12). “Crash Override”: The Malware That Took Down a Power Grid. *Wired*. Retrieved from https://www.wired.com/story/crash-override-malware/

Greenberg, A. (2017, June 20). How An Entire Nation Became Russia’s Test Lab for Cyberwar. *Wired*. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/

Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Griffiths, J. L. (2016). Cybersecurity as an emerging challenge to South African national security. *University of Pretoria*. Retrieved from https://repository.up.ac.za/bitstream/handle/2263/62639/Griffiths_Cyber_2017.pdf?sequence=1

Grigsby, A. (2015, January 28). Will China and Russia’s Updated Code of Conduct Get More Traction in a Post-Snowden Era? *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era

Grigsby, A. (2018, August 27). Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No? *Council on Foreign Relations*Retrieved from https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no

Grigsby, A. (2018, October 29). Unpacking the Competing Russian and U.S. Cyberspace Resolution at the United Nations. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations

Grigsby, Alex. (2018, November 15). The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased

Grisby, A. (2014, December 11). Coming Soon: Another Country to Ratify the Budapest Convention. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/coming-soon-another-country-ratify-budapest-convention

Grobler, M., Zaaiman, J., & Vuuren, J. C. J. van. (2013). Evaluating cyber security awareness in South Africa. *Council for Scientific and Industrial Research; University of Venda.*

Guthrie, S. (2018, September 21). Data Manipulation – a Propaganda Weapon. *Internews*. Retrieved from https://www.internews.org/news/data-manipulation-propaganda-weapon

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*. Retrieved from https://ieeexplore.ieee.org/abstract/document/7497780

Haggard, S., & Lindsay, J. R. (2015). *North Korea and the Sony hack : exporting instability through cyberspace* [report]. Honolulu, HI : East-West Center. Retrieved from http://scholarspace.manoa.hawaii.edu/handle/10125/36444

Hakmeh, J. (2017, June 6). Building a Stronger International Legal Framework on Cybercrime. Retrieved from https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime

Heller, N. (2017). Estonia, the Digital Republic. *The New Yorker.* Retrieved from https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

Herman, A. (2018, September 24). A National Cybersecurity Strategy: Better Late Than Never. *Forbes.* Retrieved from https://www.forbes.com/sites/arthurherman/2018/09/24/a-national-cybersecurity-strategy-better-late-than-never/

Hern, A. (2017, May 8). Macron hackers linked to Russian-affiliated group behind US attack. *The Guardian*. Retrieved from https://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2), (pp. 49–60). Retrieved from https://www.jstor.org/stable/pdf/26463926.pdf

Hickock, E., & Basu, A. (2018). Cyberspace and External Affairs: A Memorandum for India. *The Centre for Internet and Society.* Retrieved from https://cis-india.org/internet-governance/files/cyberspace-and-external-affairsHow Estonia became a global heavyweight in cybersecurity. (2017, June). *Invest in Estonia.* Retrieved from https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

Higgins, K. J. (2012, July 30). Iranian CERT Takes Center Stage With Flame. Dark Reading. Retrieved from https://www.darkreading.com/attacks-breaches/iranian-cert-takes-center-stage-with-fla/240001228

Hilpert, H. G. (2018). Facets of the North Korea Conflict. Actors, Problems and Europe's Interests (pp. 88). Retrieved from https://www.loc.gov/resource/frdcstdy.northkoreacountr00word/?sp=261

Hosken, G. (2014, November 13). Gautrain heist foiled. *Times Live News.* Retrieved from https://www.timeslive.co.za/news/south-africa/2014-11-13-gautrain-heist-foiled/

Ignatius, D. (2017, October 24). Russia is pushing to control cyberspace. We should all be worried. *The Washington Post.*

Indian - Computer Emergency Response Team. (n.d.). Retrieved from https://www.cert-in.org.in/

Ingber, S. (2019, February 11). Russia is considering an experiment to disconnect from the internet. *National Public Radio.*

International Law on Cyber Warfare - Tallinn Manual on the International Law Applicable to Cyber Warfare Launch. (2015). Retrieved from https://www.chathamhouse.org/file/international-law-cyber-warfare-tallinn-manual-international-law-applicable-cyber-warfare.

International Telecommunication Union Digital Inclusion Division. (2018, October 16). French Government Launched a Set of Initiatives to Promote Digital Inclusion. Retrieved from http://digitalinclusionnewslog.itu.int/2018/10/16/french-government-launched-a-set-of-initiatives-to-promote-digital-inclusion/

International Telecommunication Union. (2017). *2017 Global ICT Development Index.* Retrieved from http://www.itu.int/net4/ITU-D/idi/2017/index.html

International Telecommunication Union. (2017). China - Economy Card. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&CHN

International Telecommunication Union. (2017). Estonia - ICT Development Index 2017. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&EST

International Telecommunication Union. (2017). Global ICT Development Index. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html

International Telecommunication Union. (2017). *ICT Development Index 2017*. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&IND

International Telecommunication Union. (2017). South Africa. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&ZAF

International Telecommunication Union. (2018). Estonia - ICT Profile. Retrieved from https://www.itu.int/net4/itu-d/icteye/CountryProfileReport.aspx?countryID=76.

International Telecommunication Union. (2018). France – Profile. Retrieved from https://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx

International Telecommunication Union. (2019). ICT Profile - Canada.

International Telecommunication Union. (2019). ICT Profile – USA.

International Telecommunication Union. (n.d.). Country Profiles. Retrieved from http://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx
International Telecommunications Union. (2017). Germany - Economy Card. Retrieved from https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&DEU
International Telecommunications Union. (2018). Russian Federation - Profile. Retrieved from https://www.itu.int/net4/itu-d/icteye/CountryProfile.aspx
Internet Governance Forum. (2018, October 8). IGF 2018 Evolution of Internet Governance. Retrieved from https://www.intgovforum.org/multilingual/content/igf-2018-evolution-of-internet-governance
Internet Governance Forum. (n.d.). *2007 Participants List.* Retrieved February 7, 2019, from http://www.intgovforum.org/cms/56-igf/2007-meetings/1853-2007-rio-participants-list
Internet Governance Forum (IGF). (n.d.) Free Software Foundation Europe. Retrieved from https://fsfe.org/activities/policy/igf/igf.en.html.
Internet Governance Forum. (n.d.). *IGF 2008 Participants List*. Retrieved February 7, 2019, from http://www.intgovforum.org/cms/index.php/component/content/article/385-hyderabad-provisional-list-of-participants
Internet Governance Forum. (n.d.). *IGF 2009 Participants List*.
Internet Governance Forum. (n.d.). *IGF 2010 Participants List.* Retrieved February 7, 2019, from http://www.intgovforum.org/cms/component/content/article/96-vilnius-2010-meeting-events/748-list
Internet Governance Forum. (n.d.). *IGF 2011 Participants List.* Retrieved February 7, 2019, from http://www.intgovforum.org/cms/component/content/article/104-general/1174-list
Internet Governance Forum. (n.d.). *IGF 2012 Participants List.* Retrieved February 7, 2019, from http://www.intgovforum.org/cms/component/content/article/114-preparatory-process/1262-igf-2012-list-of-participants
Internet Governance Forum. (n.d.). *IGF 2013 Participants List* [chart]. Retrieved February 7, 2019, from http://www.intgovforum.org/cms/2013-bali/participants-list
Internet Governance Forum. (n.d.). *IGF 2015 Participants List* [chart]. Retrieved February 7, 2019, from http://www.intgovforum.org/cms/2015-igf-joao-pessoa/igf2015-participantslist
Internet Governance Forum. (n.d.). *IGF 2017 Online Participants* [chart]. Retrieved February 7, 2019, from http://www.intgovforum.org/multilingual/igf-2017-online-participants
Internet Governance Forum. (n.d.). *Official IGF Participants List* [chart]. Retrieved from http://www.intgovforum.org/cms/images/OFFICIAL%20IGF%202009%20Participants%20List.pdf
Internet Society. (2018, September 3). Internet Society (ISOC) signs MoU with The Internet Service Providers Association of India (ISPAI) to Secure India's Internet Infrastructure [press release]. Retrieved https://www.internetsociety.org/news/press-releases/2018/internet-society-isoc-signs-mou-with-the-internet-service-providers-association-of-india-ispai-to-secure-indias-internet-infrastructure/
Iran Economy, Politics and GDP Growth Summary - The Economist Intelligence Unit. (n.d.). The Economist. Retrieved from http://country.eiu.com/Iran
Javaid, A. (2018, February 11). India to sign the Budapest Convention on cyber crime. *Hindustan Times*.
Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law*, *48*. Retrieved from https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf
Jewkes, S., & Oleg, V. (2017, March). Suspected Russia-backed hackers target Baltic energy networks. *Reuters.* Retrieved from https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5

Jun, J., LaFoy, S., & Sohn, E. (2015). *North Korea's cyber operations: strategy and responses*. Washington, DC: Center for Strategic & International Studies.

Kalra, A., & Shah, A. (2018, August 18). U.S. tech giants plan to fight India's data localisation plans. *Reuters*. Retrieved from https://uk.reuters.com/article/uk-india-data-localisation-exclusive-idUKKBN1L30CN

Kamdar, M. (2018, April 23). Do Indians Have Freedom of Speech? *Pacific Council on International Policy*. Retrieved from https://www.pacificcouncil.org/newsroom/do-indians-have-freedom-speech

Kapersky Lab. (2015, February 16). *Kaspersky Lab Discovers Equation Group: The Crown Creator of Cyber-Espionage.* Retrieved from https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

Kaplan, F. (2017, September 8). We're in an Information War With Russia. It's Time We Started Acting Like It. *Slate.* Retrieved January 26, 2019, from https://slate.com/news-and-politics/2017/09/russia-is-weaponizing-social-media.html

Kar, S. (2018, April 7). How Indian Police is being trained to tackle cybercrime. *Economic Times Tech.* Retrieved from https://tech.economictimes.indiatimes.com/news/internet/how-indian-police-is-being-trained-to-tackle-cybercrime/63652035

Keshavarz, A. (2017). Iran Cyber Capabilities. In P. J. Springer (Ed.), Encyclopedia of Cyber Warfare (pp. 154-156). Santa Barbara, CA: ABC-CLIO. Retrieved from http://link.galegroup.com/apps/doc/CX7353200121/GVRL?u=wash_main&sid=GVRL&xid=cb3539f4

Kharia, R., Sethi, A., & Sathe, G. (2018, November 9). UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm. *The Huffington Post.* Retrieved from https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/

Kim, S. (2018, February 7). Inside North Korea's Hacker Army. *Bloomberg News.* Retrieved from https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army

Kirmeier, M. (2019, February 26). Aus diesen Ländern kommen die schnellsten Cyber-Angreifer. Retrieved from https://www.it-daily.net/analysen/20700-aus-diesen-laendern-kommen-die-schnellsten-cyber-angreifer

Ko, L. (2018, June 6). North Korea as a Geopolitical and Cyber Actor. *New America*. Retrieved from https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline/

Kopfstein, J. (2015, July 17). The Feds don't need digital backdoors – they can hack you. *Aljazeera America.* Retrieved from http://america.aljazeera.com/opinions/2015/7/the-feds-dont-need-digital-backdoors-they-can-hack-you.html

Korns, S. W., & Kastenberg, J. E. (2009). Georgia's cyber left hook. *Defense Technical Information Center.* Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a636632.pdf

Kotkin, S., & Beissinger, M. R. (2014). The Historical Legacies of Communism: An Empirical Agenda. In *Historical Legacies of Communism in Russia and Eastern Europe,* (pp. 1-27). Cambridge: Cambridge University Press.

Kovacs, E. (2013, February 21). Four Chinese Government Websites Hacked by Barbaros-DZ. Retrieved from https://news.softpedia.com/news/Four-Chinese-Government-Websites-Hacked-by-Barbaros-DZ-331399.shtml

Koval, N. (n.d.). *Revolution Hacking*. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Koval_06.pdf

Kulkarni, S. (2018, August 22). Cosmos Bank's Rs 94 crore online fraud: SIT recovers money from 'accidental beneficiaries' of cyber attack. *The Indian Express.* Retrieved from

https://indianexpress.com/article/cities/pune/cosmos-banks-rs-94-crore-online-fraud-sit-recovers-money-from-accidental-beneficiaries-of-cyber-attack-5318660/
Lake, E. (2019, January 4). Managing Cyberwar With Vodka. *Bloomberg News.* Retrieved from https://www.bloomberg.com/opinion/articles/2019-01-04/managing-cyberwar-with-vodka-russia-china-u-s-meet
Laudrain, A. P. B. (2018, December 4). Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace. *Lawfare.* Retrieved from https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace
Lazarus Under The Hood. (n.d.). Kapersky Lab. Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf
Lee, D. (2018, February 16). The tactics of a Russian troll farm. *BBC News.*
Lemos, R. (2003). Bush Unveils Final Cybersecurity Plan. *CNET*. Retrieved from https://www.cnet.com/news/bush-unveils-final-cybersecurity-plan/
Letsiri, V. (2018). *Submission to the Inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in Cybersecurity*. Research ICT Africa. Retrieved from https://researchictafrica.net/wp/wp-content/uploads/2018/12/Submission-Cybersecurity-ICASA-vFINAL.pdf
Li, Chunjie. (2012, June 20). 由人肉搜索谈公民隐私权保护 [Human Flesh Search: On Protecting Individual Privacy]. aisixiang.com. Retrieved from http://www.aisixiang.com/data/54582.html
Lindsay, J. R., et al. (2015). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press.
Ling, B. M. & Ling, J. (2015, July 9). Iranian Hackers Infiltrated a Canadian Government System. *VICE News.* Retrieved from https://news.vice.com/en_us/article/pa4dxm/iranian-hackers-infiltrated-a-canadian-government-system
Liu, Q.. (2018, December 29). 网络安全教育从娃娃抓起 [Cybersecurity Education Begins with Childhood]. Cyberspace Administration of China. Retrieved from http://www.cac.gov.cn/2018-12/29/c_1123924724.htm
Ljunggren, D. (2018, April 24). G7 tells tech firms to boost efforts to combat extremism: Canada. *Reuters.* Retrieved from https://www.reuters.com/article/us-g7-summit-security/g7-tells-tech-firms-to-boost-efforts-to-combat-extremism-canada-idUSKBN1HV21V
Loppie, S., Reading, C & de Leeuw, Sarah. (2014). Aboriginal Experiences with Racism and its Impacts. *National Collaborating Centre for Aboriginal Health*.
Luiijf, E., Besseling, K., & Graaf, P. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection*, 9(1). Retrieved from https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies
Lynch, S. (2018, November 29). U.S. indicts Iranian hackers responsible for deploying "SamSam". *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-iran-sanctions-idUSKCN1NX1Y3
Lyngaas, S. (n.d.). State Department to double cyber defense aid to Ukraine. Retrieved from https://www.cyberscoop.com/state-department-ukraine-cyber-aid/
MacFarquhar, N. (2018, May 15). Putin Opens Bridge to Crimea, Cementing Russia's Hold on Neighbor. *The New York Times.* Retrieved from https://www.nytimes.com/2018/05/15/world/europe/putin-russia-crimea-bridge.html
MacLellan, S., & O'Leary, N. (2017). Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game. *Centre for International Governance Innovation.* Retrieved from

https://www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game

Major Cyber Attacks on India - 2018. (2018, August 23). *Testbytes.* Retrieved from https://www.testbytes.net/blog/cyber-attacks-on-india-2018/

Makuch, B. (2016, January 25). Canada Discovers It's Under Attack by Dozens of State-Sponsored Hackers. *VICE News*. Retrieved from https://news.vice.com/en_us/article/a394pj/canada-discovers-its-under-attack-by-dozens-of-state-sponsored-hackers

Mamabolo, M. (2017, May 19). South Africa, Ivory Coast top list of African WannaCry ransomware targets. *ITWeb.* Retrieved from http://www.itwebafrica.com/security/513-africa/237876-south-africa-ivory-coast-top-list-of-african-wannacry-ransomware-targets

Mandiant. (2004). *APT 1: Exposing One of China's Cyber Espionage Units.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Manjoo, F. (2018, January 20). Saudi Money Fuels the Tech Industry. It's Time to Ask Why. *The New York Times*. Retrieved from https://www.nytimes.com/2017/11/06/technology/unsavory-sources-money-fueling-tech.html

Mansourov, A. (2014, December 2). North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance. *Korea Economic Institute of America*, 17.

Marczak, B., Scott-Railton, J. McKune, S., Razzak, B. A., Deibert, Ron. (2018, September 18). Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Retrieved from https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Markoff, J. (2008, August 12). Before the gunfire, cyber attacks. *The New York Times.*

Markoff, J. (2010, July 20). Cyberattack on Google Said to Hit Password System. *The New York Times*. Retrieved from https://www.nytimes.com/2010/04/20/technology/20google.html

Markoff, M. (2017). *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security* [statement]. Government of the United States. Retrieved from https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/GGE_2017+US+State+Department+Position.pdf

Mascolo, G. (2019, January 16). SO will der deutsche Staat Hacker stoppen. *Sueddeutsche Zeitung*. Retrieved from https://www.sueddeutsche.de/digital/cyberabwehr-plus-doxing-orbit-bka-bsi-1.4290450

Matsakis, L. (2018, December 11). The US sits out an international agreement. *Wired*. Retrieved from https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/

Maurer, T. (2016, February 5). The New Norms: Global Cyber-Security Agreements Face Challenges. *Carnegie Endowment for International Peace*. Retrieved from https://carnegieendowment.org/2016/02/05/new-norms-global-cyber-security-agreements-face-challenges-pub-63031

Maurer, T. (n.d.). *Cyber Proxies and the Crisis in Ukraine*, 10. NATO Cooperative Cyber Defence Centre of Excellence.

Mbatha, A. (2018, September 5). South Africa's ANC Worried About Electoral Support Amid Recession. *Bloomberg News.* Retrieved from https://www.bloomberg.com/news/articles/2018-09-05/s-africa-s-anc-worried-about-electoral-support-amid-recession

Mbatha, A., & Monteiro, A. (2018, July 25). South Africa gives China platform on trade as Brics meet. *Fin24.* Retrieved from https://www.fin24.com/Economy/south-africa-gives-china-platform-on-trade-as-brics-meet-20180725

McCarthy, T. (2015, February 23). NSA director defends plan to maintain "backdoors" into technology companies. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies

McFaul, M., Petrov, N., & Ryabov, A. (2010). *Between Dictatorship and Democracy: Russian Post-Communist Political Reform.* Washington, DC: The Brookings Institute Press.

McGuinness, D. (2017). How a cyber attack transformed Estonia. *BBC News*. Retrieved from https://www.bbc.com/news/39655415

McGuinness, R. (2018a, June 22). EU is at a crossroads over migrant crisis, warns French immigration chief. Retrieved from https://www.express.co.uk/news/world/978257/eu-migrant-crisis-france-immigration-latest

McGuinness, R. (2018b, August 20). Macron OUT OF STEP over migrant crisis as poll reveals HALF of French public against him. Retrieved from https://www.express.co.uk/news/world/1005956/france-news-emmanuel-macron-migrant-crisis

Merelli, A. (2018, March 8). The West is way behind Iran and Saudi Arabia when it comes to women in science. Quartz. Retrieved from https://qz.com/1223067/iran-and-saudi-arabia-lead-when-it-comes-to-women-in-science/

Meyer, D. (2018, November 12). What Is the "Paris Call?" Google and Microsoft Back Emmanuel Macron's New Plan to Protect the Internet. *Fortune Magazine.* Retrieved from http://fortune.com/2018/11/12/paris-call-google-microsoft-internet/

Ministry for Europe and Foreign Affairs. (2017, December). International Digital Strategy. Government of France. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy/

Ministry for Europe and Foreign Affairs. (2018a, June). France's role in the North Atlantic Treaty Organization (NATO). Government of France. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/france-and-nato/

Ministry for Europe and Foreign Affairs. (2018b, November). Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. Government of France. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

Ministry for Europe and Foreign Affairs. (2018c, November 12). Paris Call for Trust and Security in Cyberspace. French Government. Government of France. Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Ministry for Europe and Foreign Affairs. (2019a, February). France's International Action Against Terrorism. Government France. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/france-s-international-action-against-terrorism/

Ministry for Europe and Foreign Affairs. (2019b, January). France and Cyber security. Government of France. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/

Ministry of Communication and Information Technology. (2013, July 2). *National Cyber Security Policy – 2013* [notification]. Government of India. Retrieved from https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

Ministry of Defence. (2011, February). *National Defence Strategy Estonia.* Government of Estonia. Retrieved from http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf

Ministry of Electronics & Information Technology. (2018, April 9*). Indian Computer Emergency Response Team Annual Report 2017* [report]. Government of India.
Ministry of Electronics and Information Technology - Government of India. (n.d.). Retrieved from https://meity.gov.in/
Ministry of Electronics and Information Technology. (2017). *Active MoUs.* Government of India. Retrieved from http://meity.gov.in/content/active-mous
Ministry of Electronics and Information Technology. (2018). *Cyber Surakshit Bharat Program.* Government of India. Retrieved from https://meity.gov.in/writereaddata/files/Cyber_Surakshit_Bharat_Programme.pdf
Ministry of Electronics and Information. (2019, Feb 22). *Digital India Programme.* Government of India. Retrieved from https://digitalindia.gov.in/content/about-programme
Ministry of Foreign Affairs. (2018, November 6). *Second Ukraine – U.S. Cybersecurity Dialogue takes place at Ukraine's Foreign Ministry* [press release]. Government of Ukraine. Retrieved from https://mfa.gov.ua/en/press-center/news/68316-mzs-ukrajini-vidbuvsya-drugij-raund-mizhvidomchih-ukrajinsyko-amerikansykih-konsulytacij-u-sferi-zabezpechennya-kiberbezpeki
Ministry of Law and Justice. (2009, February 9). *The Information Technology (Amendment) Act, 2008*. Government of India. Retrieved from http://meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf
Ministry of National Defence. (2017). *Strong, Secure, Engaged: Canada's Defence Policy* [report]. Government of Canada. Retrieved from http://publications.gc.ca/collections/collection_2017/mdn-dnd/D2-386-2017-eng.pdf
Miridakis, V. (2019, January). Cyber-Attacken auf Deutsche Industrie. *It-daily.net*. Retrieved from https://www.it-daily.net/analysen/20053-cyber-attacken-auf-deutsche-industrie
Monaghan, A. (2012). The vertikal: power and authority in Russia. *International Affairs (Royal Institute of International Affairs 1994–),* 88(1), (pp. 1-16).
Mooney, C. (2018, June 1). Trump withdrew from the Paris climate deal a year ago. Here's what has changed. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/energy-environment/wp/2018/06/01/trump-withdrew-from-the-paris-climate-plan-a-year-ago-heres-what-has-changed/?utm_term=.f802faab41ff
Moran, M. (2009, March 12). French Military Strategy and NATO Reintegration. *Council of Foreign Relations.* Retrieved from https://www.cfr.org/backgrounder/french-military-strategy-and-nato-reintegration
Moses, A. (2008, August 12). Georgian websites forced offline in 'cyber war.' *The Sydney Morning Herald.*
Mumbai, A. A. (2013, July 31). How did Estonia become a leader in technology. *The Economist.* Retrieved from https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology
Museum of Public Relations. (2015, November 17). France, America's First Ally. Retrieved from http://www.prmuseum.org/blog/2015/11/17/france-americas-first-ally
Myong Hak Jong. (2016). United Nations Convention to Combat Desertification Knowledge Hub. Retrieved from https://knowledge.unccd.int/focal-points/myong-hak-jong
Nakashima, E. (2018, January 12). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?noredirect=on&utm_term=.80ab5ca6741b

Nakashima, E. Miller, G. & Tate, J. (2012, June 19). U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

Nandikotkur, G. (2015, April 13). India Opens Cyber Coordination Centre. Retrieved https://www.bankinfosecurity.asia/india-opens-cyber-coordination-centre-a-8100

National Critical Information Infrastructure Protection Centre - Government of India. (2019, February 21). Retrieved from http://nciipc.gov.in/

National Cyber Threat Assessment: 2018. (2018). Canadian Centre for Cybersecurity.

National Government of South Africa. (2019). State Information Technology Agency (SITA). Retrieved from https://nationalgovernment.co.za/units/view/187/state-information-technology-agency-sita

National Institute of Standards and Technology. (2014). Guide for applying the risk management framework to federal information systems : a security life cycle approach. Retrieved from https://doi.org/10.6028/NIST.SP.800-37r1

National Security Concept of Estonia. (2010, May 12). Government of Estonia. Retrieved from http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_of_estonia.pdf

Newton, M. & Summers, J. (2018, February 28). Russian data localization laws: Enriching "security" & the economy. *The Henry M. Jackson School of International Studies.* Retrieved from https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/

Nielsen, N. (2017, June 14). France and UK Forge Online Counter-terror Plan. *EU* Observer. Retrieved from https://euobserver.com/justice/138223

Nix, N. (2018, October 4). Why Pentagon Cloud-Computing Contract Is a Huge Deal. *Bloomberg News*. Retrieved from https://www.bloomberg.com/news/articles/2018-10-04/why-pentagon-cloud-computing-contract-is-a-huge-deal-quicktake

Nocetti, J. (2015). Contest and conquest: Russian and global internet governance. *International Affairs,* 91(1), (pp. 111-130). Retrieved from https://doi.org/10.1111/1468-2346.12189

North Atlantic Treaty Organization (NATO). (2008, May 14). NATO opens new centre of excellence on cyber defence. Retrieved from https://www.nato.int/docu/update/2008/05-may/e0514a.html

North Atlantic Treaty Organization. (2018, July 16) *Cyber defence.* Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

North Atlantic Treaty Organization. (2018, October 29). *Enhancing cybersecurity in Ukraine.* Retrieved from http://www.nato.int/cps/en/natohq/news_159840.htm

North Atlantic Treaty Organization. (2018, February 27). 10 things you need to know about NATO. Retrieved from https://www.nato.int/cps/en/natohq/126169.htm

North Atlantic Treaty Organization. (2018, July 16). Cyber defence [NATO News and Information]. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

North Korea Profile. (2018, January 5). Freedom in the World 2018. Retrieved February 10, 2019, from https://freedomhouse.org/report/freedom-world/2018/north-korea

Nossiter, A., Sanger, D. E., & Perlroth, N. (2017, May 9). Hackers Came, but the French Were Prepared. *The New York Times.* Retrieved from https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html

NSA tapped German Chancellery for decades, WikiLeaks claims. (2015, July 8). *The Guardian.* Retrieved from https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel

O'Hanlon, M. (2017). *Beyond NATO: A New Security Architecture for Eastern Europe.* Washington, DC: Brookings Institution Press.

O'Neill, P. H. (2017, July 10). NATO extends cybersecurity help to Ukraine in wake of cyberattack. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved January 25, 2019, from https://www.cyberscoop.com/nato-ukraine-cyberattack-vladimir-putin/

Office of the Secretary of Defense. (2015). Military and Security Developments Involving the Democratic People's Republic of Korea [report]. Government of the United States. Retrieved from https://dod.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF

Olejnik, L. (2019, January 22). The French doctrine of offensive cyber operations. Retrieved from https://blog.lukaszolejnik.com/the-french-doctrine-of-offensive-cyber-operations/

Organisation for Economic Co-operation and Development (OECD). (2012). *Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the Internet economy*. Paris.

Orji, U. J. (2015). Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation? (pp. 105-118). *Cyber Conflict: Architectures in Cyberspace, 2015 7th International Conference*.

Osborne, C. (2018, June 11). North Korea's history of bold cyber attacks - Page 4. Retrieved February 20, 2019, from https://www.zdnet.com/pictures/north-koreas-history-of-bold-cyber-attacks/4/

Overview - Public Private Partnerships in India. (2018). Retrieved from https://www.pppinindia.gov.in/overview

Paganini, P. (2015, July 8). Animal Farm APT and the Shadow of French Intelligence. Retrieved from https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/#gref

Pallin, C. V. (2017). Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, 33(1), (pp. 16-33). Retrieved from https://doi.org/10.1080/1060586X.2015.1121712

Panda, A. (2018, September 9). What the Recently Concluded US-India COMCASA Means. *The Diplomat*. Retrieved from https://thediplomat.com/2018/09/what-the-recently-concluded-us-india-comcasa-means/

Paris Call for Trust and Security in Cyberspace. (2019, January 23). *Liste des soutiens a l'appel de paris*. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Paris Peace Forum: furthering good governance. (2018, September 24). Government of France. Retrieved from https://www.gouvernement.fr/en/paris-peace-forum-furthering-good-governance

Paris Peace Forum. (2018). Global Platform for Governance Projects. Retrieved from https://parispeaceforum.org/program/

Park, J., & Pearson, J. (2014, December 5). In North Korea, hackers are a handpicked, pampered elite. *Reuters*. Retrieved from https://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205

Parliament of Canada. (2018, June 19). *Government Bill (House of Commons) C-59 (42-1) - Third Reading - An Act respecting national security matters*. Retrieved from http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading

Pasic, A. & Masemann, A. (Producers). (2018, February 20) How safe are Canada's elections from fake news on Facebook? *CBC Radio*. Retrieved from https://www.cbc.ca/radio/thecurrent/the-current-for-february-20-2018-1.4542333/how-safe-are-canada-s-elections-from-fake-news-on-facebook-1.4542346

Patil, S. (2018, August 15). India's lead on cyber space governance. *Indian Council on Global Relations.* Retrieved from https://www.gatewayhouse.in/india-cyber-space-governance/

Perlroth, N. (2012, October 23). Cyberattack on Saudi Oil Firm Disquiets U.S. The New York Times. Retrieved from https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Perlroth, N. (2018, May 12). Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks. The New York Times. Retrieved from https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html

Perlroth, N., & Benner, K. (2018, November 29). Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta. *The New York Times.* Retrieved from https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html

Perlroth, N., & Scott, S. (2017, October 10). How Israel caught Russian hackers scouring the world for U.S. secrets. *The New York Times.*

Pernik, P., & Tuohy, E. (2014). Interagency Cooperation on Cyber Security: The Estonian Model. In Effective Inter-Agency Interactions and Governance in Comprehensive Approaches to Operations, NATO STO Symposium Proceedings AC/323 (HFM-236) TP/579.

Peter, L. (2018, February 3). Putin, power and poison: Russia's elite FSB spy club. *BBC News.*

Pinnell, O. (2018, June 3). The online war between Qatar and Saudi Arabia. *BBC News.* Retrieved from https://www.bbc.com/news/blogs-trending-44294826

Plantera, F. (2018, October). NATO CCDCOE – Expertise and cooperation make our cyber space safer. *E-Estonia*. Retrieved from https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

Plohmann, D. (2014). SNOWGLOBE (Threat Actor): aka Animal Farm [Malware Investigation]. Retrieved from https://malpedia.caad.fkie.fraunhofer.de/actor/snowglobe

Pomerleau, M. (2018, May 18). Cyber Command reaches critical staffing milestone. Retrieved from https://www.fifthdomain.com/dod/cybercom/2018/05/17/cyber-commands-cyber-warriors-hit-key-milestone/

Pomerleau, M. (2018, October 1). How the US cyber force is maturing. Retrieved from https://www.fifthdomain.com/dod/cybercom/2018/10/01/how-the-us-cyber-force-is-maturing/

Poroshenko, P. (2016, March 16). *Cyber Security Strategy of Ukraine*. Presidential Decree No. 96/2016. Retrieved from http://ccdcoe.com/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf

President's 'cybersecurity moonshot': Will it work? (2018, December 4). Synopsis. Retrieved January 26, 2019, from https://www.synopsys.com/blogs/software-security/cybersecurity-moonshot/

Press and information team of the Delegation to the African Union. (2018, April 12). African Union Commission and Council of Europe Join Forces on Cybersecurity. Retrieved from https://eeas.europa.eu/generic-warning-system-taxonomy/404_en/42974/African%20Union%20Commission%20and%20Council%20of%20Europe%20Join%20Forces%20on%20Cybersecurity

Protalinski, E. (2012, April 4). Anonymous hacks hundreds of Chinese government sites. *ZD Net*. Retrieved from https://www.zdnet.com/article/anonymous-hacks-hundreds-of-chinese-government-sites/

Public Safety Canada. (2017, October 10). *Horizontal Evaluation of Canada's Cyber Security Strategy Final Report* [report]. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx

Public Safety Canada. (2018, June 12) *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age* [report]. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s31

Pulwama attack aftermath: Over 200 Pakistani websites hacked by Indian group. (2019, February 17). *Times Now News*. Retrieved from https://www.timesnownews.com/india/article/pakistani-websites-hacked-pulwama-attack-crpf-jawans/367541

Qatar state news agency's hacking linked to Riyadh. (2018, June 4). *Aljazeera America.* Retrieved from https://www.aljazeera.com/news/2018/06/qatar-state-news-agency-hacking-linked-riyadh-180604065614055.html

Rapoza, K. (2019, January 8). Further Investigations Show Ties of China's Huawei To Iran. *Forbes*. Retrieved from https://www.forbes.com/sites/kenrapoza/2019/01/08/further-investigations-show-chinas-huawei-broke-iran-sanctions/

Reichmann, D. (2018). U.S. on Lookout for Possible Iranian Cyber Attacks After Reinstatement of Sanctions. *Insurance Journal*. Retrieved from https://www.insurancejournal.com/news/national/2018/08/13/497767.htm

Reuters. (2017, October 6). Iran's tech startups are doing great despite sanctions. Retrieved from https://nypost.com/2017/10/06/irans-tech-startups-are-doing-great-despite-sanctions/

Reynolds, C. (2018, October 15). More than 1 in 5 businesses hit by cyberattacks last year: Statcan survey. *The Globe and Mail.* Retrieved from https://www.theglobeandmail.com/business/article-businesses-spent-14-billion-on-cybersecurity-in-2017-statistics/

Reynolds, C. (2018, October 15). More than 1 in 5 Canadian companies hit by cyberattack in 2017: StatCan. *Global News.* Retrieved from https://globalnews.ca/news/4551428/cyberattack-canadian-companies-statistics-canada/

Roane, B. (2013, May 22). SAPS website hacked. *IOL News.* Retrieved from https://www.iol.co.za/news/saps-website-hacked-1520042#.VHrpBdKUdwo

Robinson, N., Gribbon, L., Horvath, V., & Cox, K. (2013). Cyber-security threat characterisation. *RAND Europe.* Retrieved from https://www.rand.org/pubs/research_reports/RR235.html

Rodríguez, M. (2017). *Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* [statement]. Government of Cuba. Retrieved from https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/GGE_2017+Cuban-Expert-Declaration.pdf

Rollins, J. W. (2015, October 16). U.S.–China Cyber Agreement. *Federation of American Scientists*. Retrieved from https://fas.org/sgp/crs/row/IN10376.pdf

Roscini, M. (2015). Chapter 11: Cyber operations as a use of force. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 233–254). Edward Elgar Publishing. Retrieved from https://www-elgaronline-com.offcampus.lib.washington.edu/view/9781782547389.00022.xml

Rubenzer, T. (Ed.). (2017). Iran. In Today's Foreign Policy Issues: Democrats and Republicans (pp. 151–161). Santa Barbara, CA: ABC-CLIO.

S.2519 - National Cybersecurity Protection Act of 2014. (2014, December 18). 113th U.S. Congress. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2519/text/pl

SA's Ramaphosa reinforces Brics relations with China, Russia. (2018, March 13). eNews Channel Africa. Retrieved from https://www.enca.com/south-africa/sas-ramaphosa-reinforces-brics-relations-with-china-russia

Sanders R. (2016, October 4). The U.S. government no longer controls the internet. *Business Insider.* Retrieved from https://www.businessinsider.com/the-us-government-no-longer-controls-the-internet-2016-10

Sandhu, K. K. (2018, May 31). India vulnerable to cyber attacks but doesn't have capacity to deal with it: Home Secretary. *India Today*. Retrieved from https://www.indiatoday.in/india/story/india-vulnerable-to-cyber-attacks-but-doesn-t-have-capacity-to-deal-with-it-home-secretary-1247247-2018-05-31

Sanger, D. E. (2018, November 12). U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks. *The New York Times.* Retrieved from https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html

Sanger, D., & Perlroth, N. (2014, March 22). N.S.A. Breached Chinese Servers Seen as Security Threat. *The New York Times.* Retrieved from https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html

Sankaran, V. (2019, January). Here's why it is unsurprising that China, the US, and Russia didn't sign the global cyber security pact. Retrieved from https://thenextweb.com/security/2018/11/13/heres-why-it-is-unsurprising-that-china-the-us-and-russia-didnt-sign-the-global-cyber-security-pact/

Sapa. (2015, February 25). Spy Cables: Threats of cyberattack on SA banks. *eNews Channel Africa.* Retrieved from https://www.enca.com/south-africa/spy-cables-threats-cyberattack-sa-banks

Schedule - Internet Governance Forum. (2017). Retrieved January 25, 2019, from https://igf2017.intgovforum.org/

Schmitt, M. (2014). "Below the threshold" cyber operations: The countermeasures response option and international law. *Virginia Journal of International Law*, 54.

Schonhofen, S. (2018, March 13). German court issues important judgment on consent and transparency in Facebook case. Retrieved from https://www.technologylawdispatch.com/2018/03/privacy-data-protection/german-court-issues-important-judgment-on-consent-and-transparency-in-facebook-case/

Scita, Jacopo. 2018. Iran and the SCO: A Long Political Gestation. *The London School of Economics and Politics Middle East Center Blog*. Retrieved from https://blogs.lse.ac.uk/mec/2018/08/30/iran-and-the-sco-a-long-political-gestation/.

Secrétariat Général de la Défense et de la Sécurité Nationale. (2017, December 15). Stratégie internationale de la France pour le numérique. Ministry for Europe and Foreign Affairs. Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf

Secrétariat Général de la Défense et de la Sécurité Nationale. (2018, February). Strategic Review of Cyber Defense [Government]. Retrieved from http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

SEEDIG 2018 Attendance statistics. (n.d.). Retrieved from https://seedig.net/seedig-2018-attendance-statistics/

Segal, D. (2018, February 4). How Bell Pottinger, P.R. Firm for Despots and Rogues, Met Its End in South Africa. *The New York Times.* Retrieved from https://www.nytimes.com/2018/02/04/business/bell-pottinger-guptas-zuma-south-africa.html

Seger, A. (2016, October 20). India and the Budapest Convention: Why not?. *Observer Research Foundation.* Retrieved from https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/

Sen, S. R. (2018, November 3). Cyber attacks becoming more frequent in India. *Hindustan Times*. Retrieved from https://www.hindustantimes.com/india-news/cyber-attacks-becoming-more-frequent-in-india/story-8Os6AtCrHzL6QCBinVQuSM.html

Shachtman, N. (2009, March 11). Kremlin Kids: We Launched the Estonian Cyber War. *Wired*. Retrieved from https://www.wired.com/2009/03/pro-kremlin-gro/

Shackelford, S. (2009). Estonia two-and-a-half years later: a progress report on combating cyber attacks. *Journal of Internet Law.* Retrieved from http://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10242/SSRN-id1499849.pdf?sequence=1&isAllowed=y

Shafqat, N., & Masood, A. (2016, January). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*. 14(8).

Shaheen, J. (2017, September 4). The Russian company that is a danger to our security. *The New York Times*

Shalal, A. (2018, August 29). Germany, seeking independence from U.S., pushes cyber security research. *Reuters*. Retrieved from https://www.reuters.com/article/us-germany-cyber/germany-seeking-independence-from-u-s-pushes-cyber-security-research-idUSKCN1LE1FX

Shane, S. (2018, November 2). Russia Isn't the Only One Meddling in Elections. We Do It, Too. *The New York Times.* Retrieved from https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html

Shanikovsky, O. (2018, May 22). How to Identify a Fake. Retrieved from https://www.stopfake.org/en/how-to-identity-a-fake/

Shepard, B. S.. (2018, November 14). U.S. Doesn't Sign Macron's Cybersecurity Pact. *Security Today.* Retrieved from https://securitytoday.com/articles/2018/11/14/us-doesnt-sign-frances-cybersecurity-pact.aspx

Sherman, J. (2018). Russia's Tightening Control of Cyberspace Within Its Borders. *Just Security*. https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/

Shtekel, M. (2018, January 4). Ukrainian hackers turn on own government to make it care about cybersecurity. *Euromaidan Press.* Retrieved from http://euromaidanpress.com/2018/01/04/ukrainian-hackers-turn-on-own-government-to-make-it-care-about-cybersecurity/

Siemens, & Deloitte. (2017). *African Digitalization Maturity Report*. Retrieved from https://www.siemens.co.za/pool/about_us/Digitalization_Maturity_Report_2017.pdf

Siemens. (2018, November 12). *Charter of Trust goes to Paris*. Siemens. Retrieved from https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/181112-SHI-CoT-goes-Paris-Presse-EN-2.pdf

Significant Cyber Incidents. (n.d.). Center for Strategic and International Studies. Retrieved February 6, 2019, from https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

Simonite, T. (2017) The Man Who Invented the World Wide Web. *Technology Review.* Retrieved from https://www.technologyreview.com/s/604069/the-man-who-invented-the-world-wide-web/

Sindelar, D. (2014, August 12). The Kremlin's troll army. *The Atlantic.*

Smeets, M. (2018, February 8). The Netherlands just revealed its cybercapacity. So what does that mean?. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/08/the-netherlands-just-revealed-its-cybercapacity-so-what-does-that-mean/?utm_term=.b333c60c8c9c

Smith, B. (2018, November 12). An important step toward peace and security in the digital world. *Microsoft*. Retrieved from https://blogs.microsoft.com/on-the-issues/2018/11/12/an-important-step-toward-peace-and-security-in-the-digital-world/

Snowglobe. (2019). *Council on Foreign Relations*. Retrieved from https://www.cfr.org/interactive/cyber-operations/snowglobe

Staff Reporter for Independent Online. (2018, June 21). South Africans losing R2.2 billion a year to cyber attacks. *Internet Online News.* Retrieved from https://www.iol.co.za/capeargus/news/south-africans-losing-r22-billion-a-year-to-cyber-attacks-15601682

Staff Writer for IT News Africa. (2013, October 15). South Africa launches National Cyber Security Advisory Council. *IT News Africa.* Retrieved from https://www.itnewsafrica.com/2013/10/south-africa-launches-national-cyber-security-advisory-council/

State Security Agency. (2015, December 7). *National Cybersecurity Policy Framework for South Africa*. South African Government Gazette No. 39475: Government of South Africa. Retrieved from http://www.governmentpublications.lib.uct.ac.za/news/national-cybersecurity-policy-framework-south-africa

State Security Agency. (2019). State Security. Retrieved from http://www.ssa.gov.za/

Stent, D. (2018). The Great Cyber Game. *New Zealand International Review*, *43*(5), (pp. 6–9).

Stokes, M., Lin, J., Hsiao, L.C. (2011, November 11). The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance. *Project 2049 Institute*. Retrieved from http://goodtimesweb.org/surveillance/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf

Stolton, S. (2018, August 24). EU Elections 2019: Critical cyberattacks loom, Estonia warns. *Euroactiv.* Retrieved from https://www.euractiv.com/section/cybersecurity/news/eu-elections-2019-critical-cyberattacks-loom-estonia-warns/

Stolton, S. (2018, November 30). Germany: Critical cyberattacks target government and military. *EURACTIV*. Retrieved from https://www.euractiv.com/section/cybersecurity/news/germany-critical-cyberattacks-target-government-and-military-networks/

Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, 2(2), (pp. 147–184). https://doi.org/10.1007/s41125-017-0020-x

Stubbs, J. & Bing, C. (2018, November 30). Special Report: How Iran spreads disinformation around the world. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-iran-specialreport-idUSKCN1NZ1FT

Sukumar, A. (2016, May 24). Where Are US-India Cyber Relations Headed? *Lawfare*. Retrieved from https://www.lawfareblog.com/where-are-us-india-cyber-relations-headed

Sutherland, E. (2017). Governance of Cybersecurity - The Case of South Africa. *African Journal of Information and Communication* (20) (pp. 83–112). Retrieved from http://www.scielo.org.za/pdf/ajic/v20/05.pdf

Symantec. (2012). *The Elderwood Project.* Retrieved from https://www.symantec.com/connect/blogs/elderwood-project

Symantec. (2016, November). *Cyber Crime & Cyber Security Trends in Africa*. Retrieved from https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

Taher, A. (2019, January 25). Saudi Arabia's Efforts to Ensure Cyber Security. *Majalla.* Retrieved from https://eng.majalla.com/node/65466/saudi-arabia%E2%80%99s-efforts-to-ensure-cyber-security%C2%A0

Taylor, D., & Denoyelle, V. (2018, August 17). French government report on cyber threats summarized. Retrieved from https://www.limegreenipnews.com/2018/08/french-government-report-on-cyber-threats-summarized/

Technical Assistance and Information Exchange Instrument of the European Commission. (2017, October). *Expert Mission on Implementation of international standards and best practice on information security and cybersecurity.* European Neighbourhood Policy and Enlargment

Negotiations. Retrieved from https://webgate.ec.europa.eu/TMSWebRestrict/resources/js/app/#/library/detail/67106

The Cybersecurity Tech Accord endorses the Paris Call; strengthening our commitment to ensuring trust and stability in cyberspace. (2018, November 12). *Cyber Tech* Accord. Retrieved from https://cybertechaccord.org/endorses_paris_call/

The Hindu Staff Reporter. (2017, November 17). WannaCry impact on India under-reported. *The Hindu.* Retrieved from https://www.thehindu.com/news/cities/bangalore/wannacry-impact-on-india-under-reported/article20542868.ece

The Interview: A guide to the Sony Pictures hack. (2014, December 29). *BBC News.* Retrieved from https://www.bbc.com/news/entertainment-arts-30512032

The Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine. (2018, May 17). Government of Ukraine. Retrieved from http://www.dsszzi.gov.ua/dsszzi/control/en/publish/article;jsessionid=28D700BA780D085C0DE423944CC52DA7.app1?art_id=289958&cat_id=35317

The Ministry of Foreign Affairs of the Russian Federation. (2017, September 4). *Press release on signing a cooperation agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on maintaining international information security.* Government of the Russian Federation. Retrieved from http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2854430

The White House Office of the Press Secretary. (2015, January 25). *U.S.-India Joint Statement साँझा प्रयास - सबका विकास" – Shared Effort; Progress for All.* Government of the United States. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/01/25/us-india-joint-statement-shared-effort-progress-all

The White House. (2018). *National Cyber Strategy* (pp. 1-29). The Government of the United States. Washington, D.C.

Toucas, B. (2018, March 29). With its New "White Book," France Looks to Become a World-class Player in Cyber Space. Retrieved from https://warontherocks.com/2018/03/with-its-new-white-book-france-looks-to-become-a-world-class-player-in-cyber-space/

Touré, H. (2011, September 27). Speech by ITU Secretary-General, Dr Hamadoun I. Touré for the Internet Governance Forum Opening Ceremony in Nairobi, Kenya [speech]. *International Telecommunications Union.* Retrieved from https://www.itu.int/en/osg/speeches/Pages/2011-09-27.aspx

Treasury Board of Canada Secretariat. (2018, July 19). GC Information Technology Incident Management Plan [guidance]. Retrieved from https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/information-technology-incident-management-plan.html

Tripp, C. (2013). *The Power and the People: Paths of Resistance in the Middle East*. Cambridge University Press.

Troianovski, A., & Nakashima, E. (2018, December 28). How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. *The Washington Post.*

Troianovski, A., & Nakashima, E. (2018, December 28). How Russia's military intelligence agency became the covert muscle in Putin's duels with the West. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html?utm_term=.88def0f9cd7c

Tsagourias, N. & Buchan, R. (Ed.). (2015). Research Handbook on International Law and Cyberspace. Retrieved from https://www.elgaronline.com/view/9781782547389.xml

U.S. Attorney's Office Northern District of Georgia. (2015, September 29). Russian Developer of the Notorious "Citadel" Malware Sentenced to Prison [press release]. Retrieved from https://www.justice.gov/usao-ndga/pr/russian-developer-notorious-citadel-malware-sentenced-prison

U.S. Embassy Consulates in India. (2018, March 2). *Framework for the U.S.-India Cyber Relationship*. Retrieved from https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Bilateral/Framework+for+the+U.S.-India+Cyber+Relationship+8-30-2016.pdf

U.S. Embassy in Ukraine. (2017, September 29). *Embassy Statement on the First US-Ukraine Bilateral Cyber Dialogue* [press release]. U.S. State Department. Retrieved from https://ua.usembassy.gov/embassy-statement-first-us-ukraine-bilateral-cyber-dialogue/

U.S. Embassy in Ukraine. (2018, November 5). *Second U.S.-Ukraine Cybersecurity Dialogue* [press release]. U.S. Department of State Office of the Spokesperson. Retrieved February 7, 2019, from https://ua.usembassy.gov/second-u-s-ukraine-cybersecurity-dialogue/

U.S.-Canada Cybersecurity Cooperation. (2017, September 8). Retrieved from https://jsis.washington.edu/news/cybersecurity-cooperation-u-s-canada/

Uchill, J. (2018, November 12). More than 50 nations, but not U.S., sign onto cybersecurity pact. *Axios.* Retrieved from https://www.axios.com/cybersecurity-paris-call-for-trust-france-21e434df-8a59-48bc-8cde-cd1c1f43dfd0.html

Ukraine Internet Governance Forum. (n.d.). Retrieved February 20, 2019, from http://igf-ua.org/en/

Ukraine to block Russian social networks. (2017, May 16). *BBC News.* Retrieved from https://www.bbc.com/news/world-europe-39934666

UN GGE. (n.d.). *Digital Watch Observatory*. https://dig.watch/processes/ungge.

UN Office for South-South Cooperation. (2017, October 18). India, Brazil and South Africa Sign Agreement for Continued Contributions to the IBSA Fund. Retrieved from https://www.unsouthsouth.org/2017/10/18/india-brazil-and-south-africa-sign-agreement-for-continued-contributions-to-the-ibsa-fund/

United Nations General Assembly. (2011, September 12). *Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General* [letter]. Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E.

United Nations General Assembly. (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* [report]. Retrieved from https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/UNGROUP-2013.pdf.

United Nations General Assembly. (2016, October 24). *Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race* [press release]. Retrieved from https://www.un.org/press/en/2016/gadis3560.doc.htm

United Nations General Assembly. (2017). *Developments in the field of information and telecommunications in the context of international security (Report of the Secretary-General No. Seventy-second session)* [report]. Retrieved from https://undocs.org/A/72/315

United Nations General Assembly. (2018, November 15). Third Committee Approves 6 Drafts on Child Marriage, Fighting Nazi Glorification amid Discord over Long-Agreed Reproductive Rights Language, Politicized Motives [meeting coverage]. Seventy-Third Session, 48th and 49th Meetings. Retrieved from https://www.un.org/press/en/2018/gashc4253.doc.htm

United Nations Institute for Disarmament Research. (2016). Report of the International Security Cyber Issues Workshop Series [report]. Retrieved from http://www.unidir.ch/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf.

United Nations Office for Disarmament Affairs. (2019). *Developments in the Field of Information and Telecommunications in the Context of International Security* [fact sheet]. Retrieved from https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/07/Information-Security-Fact-Sheet-July2018.pdf.

US will "never recognise Russia's annexation of Crimea." (2018, July 25). *Aljazeera.* Retrieved from https://www.aljazeera.com/news/2018/07/recognise-russia-annexation-crimea-180725190209701.html

Usmanov, J. (2018, June). "The Shanghai Cooperation Organization: Harmony or Discord?" *The Diplomat*. https://thediplomat.com/2018/06/the-shanghai-cooperation-organization-harmony-or-discord/.

Vancraen, L. (2015, June 6). How to Kick-Start Ukraine's Rule of Law. *Vox News.* Retrieved from https://voxukraine.org/en/how-to-kick-start-ukraines-rule-of-law/

Wagner, M., Masters, J., & Rocha, V. (2018, July 13). Trump attends NATO summit. *CNN News.* Retrieved from https://www.cnn.com/politics/live-news/trump-nato-summit-2018/h_a49c1b87a3516e0a73ba7abeb9eeded0

Wang, Yuzhou. (2018, May 7). 坚定道路自信理直气壮抵制历史虚无主义 [Be Firm with Path Confidence Against Historical Nihilism]. Retrieved from http://www.zgdsw.org.cn/n1/2018/0507/c398751-29969190.html

Warrick, J. (2014). The United States and Israel Launched a Cyber Attack Upon Iran. In N. Berlatsky (Ed.), Cybercrime (pp. 152–157). Detroit, MI: Greenhaven Press.

Was ist Doxxing. (2019, January 4). *Frankfurter Allgemeine.* Retrieved from https://www.faz.net/aktuell/wirtschaft/diginomics/hacker-angriff-auf-politiker-was-ist-doxxing-15972248.html

Wasser, L., Lyons, C., & Koczerginski, M. (2017, October). Cybersecurity – The Legal Landscape in Canada. *McMillan Cybersecurity Bulletin.* Retrieved from https://mcmillan.ca/Cybersecurity--The-Legal-Landscape-in-Canada

Waterman, S. (2017, April 20). Six big vendors dominate a fragmented federal cybersecurity market, numbers show. Retrieved from https://www.cyberscoop.com/six-big-vendors-dominate-a-fragmented-federal-cybersecurity-market-numbers-show/

What is GeekWeek V?. (2018). Retrieved from https://g33kw33k.ca/en/about.html

White House Says WannaCry Attack Was Carried out by North Korea. (2017, December 19). *CBS News*. Retrieved from https://www.cbsnews.com/news/white-house-says-wannacry-attack-was-carried-out-by-north-korea/

Williams, M. (2011, May 3). Dot KP domain assigned to Star. *North Korea Tech.* Retrieved from https://www.northkoreatech.org/2011/05/03/dot-kp-domain-assigned-to-star/

Williams, M. (2017, October 2). Russia Provides New Internet Connection to North Korea. *38 North: Informed Analysis of North Korea.* Retrieved from https://www.38north.org/2017/10/mwilliams100117/

Wolf, S. (2015, January 13). BND warnt vor Hackern des ''Islamischen Staats". *Das Erste.* Retrieved from https://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/videos-und-manuskripte/hacker-islamischer-staat-100.html

Worden, R. (2018). North Korea : a country study. Retrieved from https://www.loc.gov/item/2008028547/

World Summit on the Information Society. (2005, November 18). *Tunis Agenda for the Information Society.* Retrieved from https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

Worldometers. (2019). Countries in the world by population (2019) [data]. Retrieved from http://www.worldometers.info/world-population/population-by-country/

Yang, Linlin. (2018, May 7). "信息丝绸之路"务实延展显蓝图 [Digital Silk Road Shows Blueprint Steadily]. Cyberspace Administration of China. Retrieved from http://www.cac.gov.cn/2016-12/22/c_1120158753.htm

Yourish, K., & Griggs, T. (2018, July 16). 8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html

Zakrzewski, C. (2018, November 13). The Cybersecurity 202: The U.S. was notably absent from a global cybersecurity pact. But American companies signed on. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/11/13/the-cybersecurity-202-the-u-s-was-notably-absent-from-a-global-cybersecurity-pact-but-american-companies-signed-on/5be9c0881b326b3929054751/?noredirect=on&utm_term=.3b3da746a0be

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired*. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. (2015, February 10). The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks. *Wired*. Retrieved from https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

Zimmerman, V. (2016, April 20). Ukraine's Finally Got a Cybersecurity Strategy. But Is It Enough? *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-s-finally-got-a-cybersecurity-strategy-but-is-it-enough

Zlenko, S. (2017). *Press releases and reports - Trust to social institutions.* Kyiv International Institute of Sociology. Retrieved from http://www.kiis.com.ua/?lang=eng&cat=reports&id=678

习近平：警惕"黑天鹅"防范"灰犀牛"[Xi Jinping: Be Alert with "Black Swam" and "Grey Rhino]. (2019, January 22). *People's Daily.* Retrieved from http://money.people.com.cn/n1/2019/0122/c42877-30583468.html

勒索病毒肆虐全球 国内高校为何成病毒攻击"重灾区"[Ransomware Spread Globally: Why Chinese Universities Take the Most Hit]. (2017, May 14). *Xinhua News Agency.* Retrieved from http://www.xinhuanet.com/politics/2017-05/14/c_1120967940.htm

反共黑客网 [Anti-Communist Hacker Website]. Retrieved from http://www.fangongheike.com/

吃饭购物都可能被直播：谁在泄露我们的隐私？ [Being Livestreaming During Eating and Shopping: Who's leaking our privacy?]. (2018, April 14). *Xinhua News Agency*. Retrieved from http://www.xinhuanet.com/local/2018-04/14/c_1122680615.htm

解放军61580部队 [PLA 61580 Unit]. *Wanfang Data*. Retrieved from http://miner.wanfangdata.com.cn/unitBootPage/toUnitBootpage.do?themeWord=解放军61580部队

HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES

UNIVERSITY *of* WASHINGTON

The Henry M. Jackson School of International Studies
jsis.washington.edu | Phone: (206) 543-6001 | Email: jsis@uw.edu