



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**INTERNATIONAL GOVERNANCE OF NON-STATE  
ACTORS IN CYBERSPACE: IS A SINGLE ENTITY  
SUFFICIENT FOR DISPUTE RESOLUTION?**

by

Jaclyn L. Francis

June 2020

Co-Advisors:

Lynda A. Peters (contractor)  
Shannon A. Brown

**Approved for public release. Distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                 |                                                                |                                                            |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------|--|
| <b>REPORT DOCUMENTATION PAGE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                 |                                                                | <i>Form Approved OMB<br/>No. 0704-0188</i>                 |  |
| Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                 |                                                                |                                                            |  |
| <b>1. AGENCY USE ONLY<br/>(Leave blank)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                 | <b>2. REPORT DATE</b><br>June 2020                             | <b>3. REPORT TYPE AND DATES COVERED</b><br>Master's thesis |  |
| <b>4. TITLE AND SUBTITLE</b><br>INTERNATIONAL GOVERNANCE OF NON-STATE ACTORS IN CYBERSPACE: IS A SINGLE ENTITY SUFFICIENT FOR DISPUTE RESOLUTION?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                 |                                                                | <b>5. FUNDING NUMBERS</b>                                  |  |
| <b>6. AUTHOR(S)</b> Jaclyn L. Francis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                 |                                                                |                                                            |  |
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br>Naval Postgraduate School<br>Monterey, CA 93943-5000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                 |                                                                | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>            |  |
| <b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                | <b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>    |  |
| <b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                 |                                                                |                                                            |  |
| <b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b><br>Approved for public release. Distribution is unlimited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                 |                                                                | <b>12b. DISTRIBUTION CODE</b><br>A                         |  |
| <b>13. ABSTRACT (maximum 200 words)</b><br><p>Cyberattacks by non-state actors have evolved with the speed of technology, leaving governments largely powerless to address emerging threats, partly due to the lack of legal options to dissuade or deter malicious non-state actors. To adequately address the threat, the international community must form legally binding mechanisms to pursue non-state actors similar to the way the world rethought terrorism after 9/11. This thesis rejects a proposed dispute-mitigation recommendation now under consideration by international negotiators—the NATO Cooperative Cyber Defence Centre of Excellence, leveraging the Budapest Convention on Cybercrime as its framework—and explores an alternative approach for the international governance of the cyber domain, with due mechanisms established to address the ongoing threat of malicious non-state actors. Numerous stakeholders influence cyber strategies in the U.S. and internationally; therefore, a one-system entity is an ineffective regulatory mechanism. Rather, it should be multi-pronged, multilateral, and comprise a unified approach that includes the UN, NATO, INTERPOL, as well as sanctioned unilateral state processes to achieve optimal outcomes. The Paris Climate Agreement should be referenced as a model for success in garnering support for this governance initiative, utilizing the UN to define the space and develop a clear, well-defined framework leveraging the Budapest Convention and the <i>Tallinn Manual 2.0</i> encapsulated in an amendable treaty.</p> |                                                                 |                                                                |                                                            |  |
| <b>14. SUBJECT TERMS</b><br>cyber, international law, cyber domain, governance, non-state actors, cyber law, cyber governance, governing bodies, regulation, regulatory measures, dispute resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                 |                                                                | <b>15. NUMBER OF PAGES</b><br>135                          |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                 |                                                                | <b>16. PRICE CODE</b>                                      |  |
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>UU                    |  |

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

**INTERNATIONAL GOVERNANCE OF NON-STATE ACTORS  
IN CYBERSPACE: IS A SINGLE ENTITY SUFFICIENT  
FOR DISPUTE RESOLUTION?**

Jaclyn L. Francis  
Senior Program Manager, U.S. Customs and Border Protection,  
Department of Homeland Security  
BA, The George Washington University, 2001  
JD, Catholic University of America, 2005

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES  
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL  
March 2021**

Approved by: Lynda A. Peters  
Co-Advisor

Shannon A. Brown  
Co-Advisor

Erik J. Dahl  
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## ABSTRACT

Cyberattacks by non-state actors have evolved with the speed of technology, leaving governments largely powerless to address emerging threats, partly due to the lack of legal options to dissuade or deter malicious non-state actors. To adequately address the threat, the international community must form legally binding mechanisms to pursue non-state actors similar to the way the world rethought terrorism after 9/11. This thesis rejects a proposed dispute-mitigation recommendation now under consideration by international negotiators—the NATO Cooperative Cyber Defence Centre of Excellence, leveraging the Budapest Convention on Cybercrime as its framework—and explores an alternative approach for the international governance of the cyber domain, with due mechanisms established to address the ongoing threat of malicious non-state actors. Numerous stakeholders influence cyber strategies in the U.S. and internationally; therefore, a one-system entity is an ineffective regulatory mechanism. Rather, it should be multi-pronged, multilateral, and comprise a unified approach that includes the UN, NATO, INTERPOL, as well as sanctioned unilateral state processes to achieve optimal outcomes. The Paris Climate Agreement should be referenced as a model for success in garnering support for this governance initiative, utilizing the UN to define the space and develop a clear, well-defined framework leveraging the Budapest Convention and the *Tallinn Manual 2.0* encapsulated in an amendable treaty.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

|             |                                                                                             |           |
|-------------|---------------------------------------------------------------------------------------------|-----------|
| <b>I.</b>   | <b>INTRODUCTION.....</b>                                                                    | <b>1</b>  |
| <b>A.</b>   | <b>PROBLEM STATEMENT .....</b>                                                              | <b>1</b>  |
| <b>B.</b>   | <b>RESEARCH QUESTION .....</b>                                                              | <b>7</b>  |
| <b>C.</b>   | <b>LITERATURE REVIEW .....</b>                                                              | <b>7</b>  |
| <b>D.</b>   | <b>RESEARCH DESIGN.....</b>                                                                 | <b>13</b> |
| <b>II.</b>  | <b>CYBER THREATS AND POLICY RESPONSES.....</b>                                              | <b>15</b> |
| <b>A.</b>   | <b>POWER COMPETITION WITH CHINA, RUSSIA AND<br/>NORTH KOREA .....</b>                       | <b>15</b> |
| 1.          | China .....                                                                                 | 15        |
| 2.          | Russia .....                                                                                | 17        |
| 3.          | North Korea.....                                                                            | 18        |
| <b>B.</b>   | <b>U.S. CYBER POLICY DEVELOPMENTS .....</b>                                                 | <b>20</b> |
| <b>C.</b>   | <b>THE MAIN CYBER ACTORS .....</b>                                                          | <b>35</b> |
| 1.          | Nation-State Actors.....                                                                    | 36        |
| 2.          | Proxy State Actors .....                                                                    | 37        |
| 3.          | Non-state Actors.....                                                                       | 39        |
| <b>III.</b> | <b>RULES OF ENGAGEMENT, INTERNATIONAL LAW, AND<br/>CYBERSPACE .....</b>                     | <b>45</b> |
| <b>A.</b>   | <b>LAW OF WAR OVERVIEW .....</b>                                                            | <b>46</b> |
| <b>B.</b>   | <b>RESTATEMENT OF LAW: <i>TALLINN MANUAL 2.0</i>'S<br/>EXAMINATION.....</b>                 | <b>53</b> |
| 1.          | State Sovereignty in Cyberspace .....                                                       | 55        |
| 2.          | Due Diligence.....                                                                          | 58        |
| 3.          | Jurisdiction .....                                                                          | 59        |
| <b>C.</b>   | <b>BUDAPEST CONVENTION.....</b>                                                             | <b>62</b> |
| <b>D.</b>   | <b>NORTH ATLANTIC TREATY ORGANIZATION.....</b>                                              | <b>65</b> |
| <b>E.</b>   | <b>THE UNITED NATIONS .....</b>                                                             | <b>70</b> |
| 1.          | UN Security Council .....                                                                   | 71        |
| 2.          | The International Court of Justice.....                                                     | 72        |
| <b>F.</b>   | <b>CONCLUSION .....</b>                                                                     | <b>73</b> |
| <b>IV.</b>  | <b>IS NATO CCDCOE THE RIGHT ENTITY TO ARBITRATE<br/>CONFLICT IN THE CYBER DOMAIN? .....</b> | <b>75</b> |
| <b>A.</b>   | <b>THE PARIS CLIMATE AGREEMENT MODEL.....</b>                                               | <b>77</b> |
| <b>B.</b>   | <b>FRAMEWORK FOR DEVELOPING LEGAL STANDARDS.....</b>                                        | <b>79</b> |

|    |                                                                     |     |
|----|---------------------------------------------------------------------|-----|
| C. | MULTI-PRONGED APPROACH FOR CYBER GOVERNANCE.....                    | 81  |
| 1. | Defining the Space via the UN .....                                 | 82  |
| 2. | Diplomatic Approaches .....                                         | 83  |
| 3. | Response Capabilities in a Defined Cyber Environment .....          | 84  |
| 4. | Legal Venues .....                                                  | 88  |
| V. | RECOMMENDATIONS AND CONCLUSIONS.....                                | 91  |
| A. | COMPLIANCE AND ENFORCEMENT .....                                    | 94  |
| B. | THE UNITED STATES' ROLE IN INTERNATIONAL GOVERNANCE MECHANISMS..... | 95  |
| C. | CONCLUSION .....                                                    | 96  |
|    | LIST OF REFERENCES .....                                            | 99  |
|    | INITIAL DISTRIBUTION LIST .....                                     | 113 |

## LIST OF FIGURES

|            |                                                                                      |    |
|------------|--------------------------------------------------------------------------------------|----|
| Figure 1.  | Visual Depiction of Vulnerabilities Magnitude.....                                   | 5  |
| Figure 2.  | DOD <i>Cyber Strategy</i> Alignment with DOD Guidance.....                           | 25 |
| Figure 3.  | DHS Organizational Chart Depicting CISA (in red box) .....                           | 31 |
| Figure 4.  | CISA Regional Service Delivery Sections .....                                        | 32 |
| Figure 5.  | DOD Digital Modernization Goals (left) and Priorities (right) 2019 .....             | 35 |
| Figure 6.  | Example of the Intimidating Message in the 2014 Sony Attack .....                    | 38 |
| Figure 7.  | Main Non-state Actors in Cyberspace. ....                                            | 40 |
| Figure 8.  | Compromised U.S. CENTCOM Twitter Page.....                                           | 42 |
| Figure 9.  | List of Characteristics Comparing Cyber Domain vs. Traditional Warfare Domains ..... | 49 |
| Figure 10. | Information and Kinetic Warfare Spectrum Chart.....                                  | 50 |
| Figure 11. | Steps in Accountability for Malign Activity.....                                     | 81 |
| Figure 12. | Recommended Governance Approach .....                                                | 82 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

|          |                                                             |    |
|----------|-------------------------------------------------------------|----|
| Table 1. | State Proxy Relationships and Level of Coercive Power ..... | 37 |
|----------|-------------------------------------------------------------|----|

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS AND ABBREVIATIONS

|          |                                                  |
|----------|--------------------------------------------------|
| ACDC     | Active Cyber Defense Certainty (Act)             |
| AU       | African Union                                    |
| CCDCOE   | Cooperative Cyber Defence Centre of Excellence   |
| CDA      | Cyber Diplomacy Act of 2017                      |
| CHDS     | Center for Homeland Defense and Security         |
| CIA      | Central Intelligence Agency                      |
| CISA     | Cybersecurity and Infrastructure Security Agency |
| CFR      | Council on Foreign Relations                     |
| DHS      | Department of Homeland Security                  |
| DNI      | Director of National Intelligence                |
| DOD      | Department of Defense                            |
| EU       | European Union                                   |
| FEMA     | Federal Emergency Management Agency              |
| FBI      | Federal Bureau of Investigation                  |
| GCC      | Gulf Cooperation Council                         |
| IC       | Intelligence Community                           |
| ICC      | International Criminal Court                     |
| ICJ      | International Court of Justice                   |
| IGE      | International Group of Experts                   |
| INTERPOL | International Criminal Police Organization       |
| IO       | Information Operations                           |
| IS/ISIS  | Islamic State/Islamic State of Iraq and Syria    |
| LOW      | law of war                                       |
| NATO     | North Atlantic Treaty Organization               |
| NPDD     | National Protection and Programs Directorate     |
| NPS      | Naval Postgraduate School                        |
| NSA      | National Security Agency                         |
| OPM      | Office of Personnel Management                   |
| PLA      | People's Liberation Army                         |
| ROE      | rules of engagement                              |

|                    |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| <i>Tallinn</i>     | <i>Tallinn Manual on the International Law Applicable to Cyber Warfare</i>        |
| <i>Tallinn 2.0</i> | <i>Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations</i> |
| UN                 | United Nations                                                                    |
| USCYBERCOM         | U.S. Cyber Command                                                                |

## EXECUTIVE SUMMARY

The 21st century digital “Information Age” is characterized by dynamism, innovation, and new technological capabilities. The cyber domain provides limitless technological capabilities to improve living in the modern world. As technological capabilities expand to meet the needs of an information-driven society, it is critical that the international community create an international mechanism for effective cyber-governance to mitigate vulnerabilities and respond to threats that impact national and international security.

Cyber activities are transnational, evolve rapidly, and affect the international community’s critical infrastructure, states, cities, and localities. Most cyber activities are legitimate; they respond to people’s demands, promote economic growth, and support quality of life for many people around the world. Nation-state cyber actors are at the forefront of cyber discussions among cyber-centric international governments, the private sector, and academia. A gap, however, pertains to information about non-state actors regarding regulation, compliance, and enforcement mechanisms. The *Tallinn Manuals’* International Group of Experts (IGE) were unanimous in their estimations that cyber activities do not exist in a normative void and that existing international law applies to cyber operations. Cyber governance cannot be solely based on the concept of sovereignty, regulated by nation-states. Formal international governing mechanisms are critical for global understanding of cyberspace boundaries and a unified response to resolve cyber disputes. There are very few treaties for cyber activities and those that do exist are of limited scope and applicability. Efforts need to involve coordinated partnerships that span federal, state, and local levels in the United States; internationally; in the private sector; and with academic subject matter experts to develop and implement effective governance.

During the April 2019 Atlantic Council’s Eighth Annual International Conference on Cyber Engagement (ICCE) in Washington, DC, a group of cyber experts discussed multi-disciplinary approaches to develop international collaboration and norms to act

against growing cyberattacks.<sup>1</sup> David Koh, chief executive of Singapore’s Cyber Security Agency, advised of the need for a whole-of-government global engagement to develop a legal framework of measures and oversight; a “vibrant cybersecurity ecosystem.”<sup>2</sup> International order is necessary for the collective security of all nation-states.

This thesis arose from Isaac “Ike” Barnes’s 2018 Center for Homeland Defense and Security (CHDS) thesis. As part of his holistic approach, Barnes discussed the need for a cyber dispute mitigation entity. He identified the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCDCOE) as the entity together with the Budapest Convention on Cybercrime as the framework. Barnes’s designation of the CCDCOE as the governing body is based on the center’s history with cybersecurity; specifically its IGE, who interpreted and restated international law, contained within the *Tallinn Manuals*, as applied to the cyber domain. This thesis disputes his proposal and builds upon his effort by considering an alternative approach to international governance of non-state actors in the cyber domain. Numerous stakeholders influence cyber strategies in the United States and internationally; therefore, a one-system entity is an ineffective regulatory mechanism. Rather, an international cyber-governance mechanism should be a multi-pronged, multilateral, and unified approach to achieve the greatest success with concession by a majority of the international cyber community.

This research explored the current cyber landscape including existing international law, cyber rules of engagement (ROE), and regulatory mechanisms. Then, this study examined Barnes’s recommended future course of study for a mitigation entity in the context of non-state cyber activities. Subject matter analysis from multiple datasets provided insight into the existence, enforcement, and effectiveness of international law application to the cyber domain, as well as missing pieces in cyber international governance.

---

<sup>1</sup> Catherine Lotrionte, “Atlantic Council Eighth Annual International Conference on Cyber Engagement (ICCE): Introductory Remarks” (symposium, G.W. Lisner Auditorium, George Washington University, Washington, DC, April 22, 2019), <https://www.atlanticcouncil.org/icce>.

<sup>2</sup> David Koh, “Atlantic Council Eighth Annual International Conference on Cyber Engagement (ICCE): Keynote Address” (symposium, G.W. Lisner Auditorium, George Washington University, Washington, DC, April 22, 2019), <https://www.atlanticcouncil.org/icce>.

After reviewing Barnes's mitigation proposal, the researcher identified flaws and proposed an alternative multi-pronged regulatory mechanism solution. Numerous stakeholders influence cyber strategies in the United States and internationally; therefore, a one-system entity is an ineffective regulatory mechanism. Rather, it should be a multi-pronged, multilateral, and unified approach to achieve the greatest success, with concession by a majority of the international cyber community. The multi-pronged approach includes NATO, the International Criminal Police Organization (INTERPOL), and unilateral processes such as the Paris Climate Agreement and the United Nations (UN). The Paris Climate Agreement should be referenced as a model for success in garnering support for this major global cyber initiative, and the UN should delineate the space and develop a clear, well-defined framework using both the Budapest Convention and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0)* encapsulated in an amendable treaty. In consideration of cyberspace's rapid evolution and key players, the *Tallinn 2.0* restatements of law should be expanded to include non-state activity, either through attribution or forensic analysis to associate them with a state, for international law application. Similar to the post-World War II era establishment of international laws and norms governing conflicts between states, the United States should guide conversations to develop recommended courses of action to apply law to cyberspace, explore threats, understand their drivers and challenges, determine the best courses of action for regulatory measures and compliance, and offer suggestions for cyber-specific regulatory measures. Likewise, this thesis also recommends future areas of study to explore compliance, enforcement, and the United States' role in such an international cyber governance mechanism.

The United States is a key player in the cyber domain and needs to fully engage in governance discussions and development to ensure inclusion, intelligence and information sharing, transparency, and accountability. A key takeaway and lesson learned from the research is that the U.S. government must continue to build and improve cooperation with national and international partners, as the issue will not be resolved unilaterally. An international governing mechanism will impact global security, and concurrently, U.S. homeland security by providing clarity on cyber rules and regulation measures for

mitigation and response to malign cyber actions by non-state actors. A secure border is a multilateral, shared effort; difficulties arise when the borders are complex and activity frequently travels across state borders. The issue will not be solved quickly, yet the discussions must continue at full speed to head toward a resolution before cyberspace expands beyond our ability to regulate it. An effective multi-pronged international governance approach will be a culmination of effective coordinated partnerships and collaborative efforts to provide critical oversight and response to criminal and terrorist activity within the rapidly expanding and evolving cyber problem space. A governance mechanism will provide homeland security benefits for the United States via operational approaches, augmented responses to criminal activity, increased resources for cyber security resilience, and possible deterrence.

## ACKNOWLEDGEMENTS

Foremost, I am indebted to my family for their support and sacrifices during this 18-month master's program and thesis process. Their love kept me going and completion would not have been possible without them. Spending two weeks across the country every quarter was a disruption to routine that required patience and strength. Thank you to my husband for being understanding. Thank you to my children—mostly EH since AS wasn't born until three-quarters into the process—for their patience. Thank you to my parents for instilling in me the dedication, perseverance, and desire to learn. I would like to thank my mother, brother, sister-in-law, brother-in-law, and countless others who came through in a pinch to help out with the kids while I was in California.

I wish to express my sincere appreciation to my current and previous supervisors, Courtney Liggins and Tom Marenic, respectively, who professionally enabled and supported my participation in the NPS CHDS master's program.

My gratitude extends to my thesis committee, Lynda Peters and Shannon Brown, who entertained my ideas to shape, scope, and develop this document. They demonstrated patience, motivation, enthusiasm, and immense knowledge.

Besides my advisors, thank you to two individuals who were invaluable during the thesis process: Lauren Wollman and Marianne Taflinger. Both provided mentorship, insightful comments, hard questions, and encouragement at critical times. I am also thankful for all of the people whose assistance was a milestone in the completion of this project whether it be citation help, editing, brainstorming, and logistical support.

Finally, to the best cohort—1805/1806—thank you. I am grateful you fostered an educational environment that was insightful, thought-provoking, and a place to look forward to attending each day. We were one another's support, editors, cheerleaders, comedians, and therapists. I treasure each person I have been able to get to know on a personal level. Our classroom, off campus, and distance gatherings have been fun and unforgettable. I look forward to continuing lifelong friendships. Monterey will always hold a special place in my heart.

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION

### A. PROBLEM STATEMENT

The 21st century “Information Age” is characterized by dynamism, innovation, and new technological capabilities. The cyber domain provides limitless technological capabilities to improve living in the modern world. During a May 29, 2009, speech, President Barack Obama stated, “This world—cyberspace—is a world that we depend on every single day ... [it] has made us more interconnected than at any time in human history.”<sup>1</sup>

As technological capabilities expand to meet the needs of an information-driven society, it is critical that the international community create an international mechanism for effective cyber governance to mitigate vulnerabilities and respond to threats that impact national and international security. Advancement of information technologies, global proliferation of affordable internet access, and the subsequent weaponization of these platforms has evolved into a credible threat to international and U.S. homeland security. The United States remains the preeminent target for malicious cyber activity, ranging from cyber-enabled economic espionage to cyberattacks targeting government and private sector business interests. Recently, Richard Clarke stated that “very little has been done in the last 10 years to protect major systems (critical infrastructure) in the United States ... to protect our own military weapons systems ... to secure the government.”<sup>2</sup> We have seen firsthand the government’s lack of cyber security with the 2015 Office of Personnel Management (OPM) incidents when background investigation records and personal data of 4.2 million employees were stolen.<sup>3</sup> There were 30,899 information-security incidents reported by the federal government in 2016, 16 of which were considered major incidents; in 2017, 21

---

<sup>1</sup> Barack Obama, *Securing U.S. Cyber Infrastructure* (Washington, DC: American Rhetoric Online Speech Bank, 2009).

<sup>2</sup> A. J. Vicens, “The U.S. Government Has Done ‘Almost Nothing’ to Stop Cyber Attacks,” *Mother Jones*, July 16, 2019, <https://www.motherjones.com/politics/2019/07/the-us-government-has-done-almost-nothing-to-stop-cyber-attacks/>.

<sup>3</sup> “Cybersecurity Resource Center, What Happened,” Office of Personnel Management, accessed July 28, 2019. <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>; Vicens.

agencies continued to show vulnerabilities in five major areas of concern.<sup>4</sup> Aligning cyber operations with national and international policies is imperative to decision-making. A shift toward an international collaborative response to apply international laws and develop cyber norms presents numerous potential challenges, especially in the following areas: reaching consensus, securing adherence from countries with differing mindsets about the cyber environment, complying, and enforcing such agreements.

Internet use has grown exponentially over the years, bringing with it greater vulnerability to criminal activity. Cyberspace is the new battlefield, with state-sponsored cyberattacks resulting in devastating effects to a wide range of entities, from credit company data breaches to the Sony release of confidential data. State-sponsored cyberattacks have crippled companies, affected the economy, and jeopardized the security and privacy of companies and individuals. WannaCry, a devastating May 2017 ransomware attack linked to the North Korean state-sponsored cybercriminal organization, Lazarus Group, exploited Microsoft Windows vulnerabilities discovered—but not resolved in a timely way—by the National Security Agency (NSA).<sup>5</sup> In 2017, Cybersecurity Ventures reported the average cost of a single ransomware attack is \$5 million, including system downtime, information technology (IT) and user productivity losses, with cybercrime costs expected to hit \$6 trillion annually by 2021.<sup>6</sup> The chaos and economic losses resulting from these recent ransomware attacks have highlighted the need for an operational transformation focused on cyber deterrence.

State actors—Russia, North Korea, China, Iran—are at the forefront of cyber discussions among cyber-centric international governments, the private sector, and academia. A gap, however, pertains to information about non-state actors and proxy state actors regarding regulation, compliance, and enforcement mechanisms. Both types of

---

<sup>4</sup> Riley Walters, “Federal Cyber Breaches in 2017,” The Heritage Foundation, January 3, 2018, <https://www.heritage.org/cybersecurity/report/federal-cyber-breaches-2017>.

<sup>5</sup> Josh Fruhlinger, “What Is WannaCry Ransomware, How Does It Infect, and Who Was Responsible?” CSO, accessed November 11, 2018, <https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>.

<sup>6</sup> Steve Morgan, “Global Ransomware Damage Costs Predicted To Exceed \$5 Billion In 2017,” Cybercrime Magazine, May 18, 2017. <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/>.

actors pose interesting cyber challenges because of the difficulties of attribution. For example, proxy state actors provide a distinct governance challenge because they are purportedly acting under the arm of a state actor, but the state actor refuses to acknowledge or admit ties to those actions. This arms-length relationship raises questions about how sanctions could be applied and to whom—an individual or a group? Similar to the post-World War II era establishment of international laws and norms governing conflicts between states, the United States should guide conversations to develop recommended courses of action to apply law to cyberspace, explore each of those threats, understand their drivers and challenges, determine the best courses of action for regulatory measures and compliance, and offer suggestions for cyber-specific regulatory measures.

The 2016 U.S. presidential election represented a watermark moment for the country as the first publicly exposed instance in which a foreign state actor, by leveraging information technologies, executed a complex information campaign and cyber operations at the local, state, and national levels to influence a U.S. election. While subsequent criminal investigations are ongoing, the ability to leverage the cyber domain as a tool to influence public opinion by exploiting public- and private-sector protected data through multiple delivery vehicles via the internet is a critical national security concern.

On January 6, 2016, the Office of the Director of National Intelligence ODNI released a declassified report, stating that the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and NSA have “high confidence” that Russian President Vladimir Putin ordered activities to influence the U.S. presidential election in order to “undermine public faith in the U.S. democratic process, denigrate [Hillary] Clinton, and harm her electability and potential presidency.”<sup>7</sup> These activities were facilitated “by cyber-espionage and cyber-driven covert influence operations, conducted as

---

<sup>7</sup> Richard Burr, “Senate Select Committee on Intelligence,” [burr.senate.gov](https://www.burr.senate.gov/download/final-ssci-ica-assessment), July 3, 2018, <https://www.burr.senate.gov/download/final-ssci-ica-assessment>; Catherine A. Theohary and Cory Welt, “Russia and the U.S. Presidential Election,” Congressional Research Service, January 17, 2017. <https://fas.org/sgp/crs/natsec/IN10635.pdf>.

part of a broader ‘active measures’ campaign that included overt messaging through Russian-controlled propaganda platforms.”<sup>8</sup>

Prior work by the U.S. Intelligence Community (IC) and interagency programs provided warnings of potential operations, but the scope of these cyberattacks is still not completely understood. What is clear is the need to address the threats that the cyber environment presents to U.S. interests in both the national and international arenas to successfully mitigate cyber vulnerabilities and secure the U.S. homeland. Cyber operations present a high-yield, low-cost option with deniability and entity-masking that will make future attacks against the United States by proxy state and non-state actors a viable option. Not all cyberattacks involve high-profile critical infrastructure targets; many attacks are executed on lightly defended targets of opportunity such as outdated security updates, incompetent or unknowing users who click on malicious links, or social engineering that can all be done through a simple phone call or by entering default passwords.<sup>9</sup> An October 2018 U.S. Government Accountability Office (GAO) report employed test teams to detect mission-critical vulnerabilities in weapons systems that were under development. Using basic, simple tools and techniques that require “little knowledge or expertise,” testers easily gained unauthorized, undetected access and control; one team indicated an administrative password was guessed in nine seconds.<sup>10</sup> Although testing uncovers basic to moderate vulnerabilities, the majority of extensive, sophisticated vulnerabilities likely exist deeper under the surface, beyond current testing simulation (see Figure 1).<sup>11</sup>

---

<sup>8</sup> “Senate Select Committee on Intelligence,” U.S. Senate, July 3, 2018, <https://www.intelligence.senate.gov/publications/committee-findings-2017-intelligence-community-assessment>.

<sup>9</sup> Alex Hern, “Cyber-Attacks and Hacking: What You Need To Know,” *Guardian*, November 1, 2016, <https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime>.

<sup>10</sup> U.S. Government Accountability Office, *Weapons Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC: Government Accountability Office, 2018), 21. <https://www.gao.gov/assets/700/694913.pdf>.

<sup>11</sup> U.S. Government Accountability Office, 26.

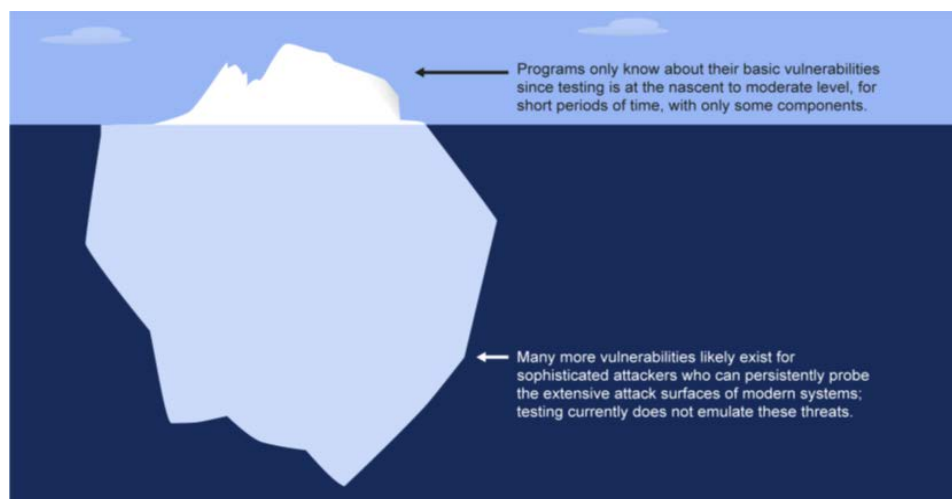


Figure 1. Visual Depiction of Vulnerabilities Magnitude<sup>12</sup>

As digital technologies enable businesses to become more adaptable and agile in the workplace, the potential increases for cybercriminals to gain access to information networks. In November 2014, the Guardians of the Peace (GOP) publicly brought North Korea into the cyber limelight when it hacked Sony in retaliation for a planned release—later, canceled—of a comedy movie film centered on the assassination of a North Korean leader.<sup>13</sup> According to Dmitri Alperovitch, cofounder of cybersecurity firm CrowdStrike, the Sony incident was “the first time a country has forced a target—through a cyberattack—to change its behavior against its will.”<sup>14</sup> This incident crippled the entire corporate network, forcing business organizations to take cybercrime seriously.

As the cyber battlespace evolves and expands, it will become a premier venue for unconventional warfare. The cyber domain is not a new area of operation; the U.S. Cyber Command was created over ten years ago in 2008 (fully operational in 2010) to lead and

<sup>12</sup> Source: U.S. Government Accountability Office.

<sup>13</sup> Zach Whittaker, “FBI Says North Korea Is ‘Responsible’ For Sony Hack, As White House Mulls Response,” ZDNet, December 19, 2014, <https://www.zdnet.com/article/us-government-officially-blames-north-korea-for-sony-hack/>.

<sup>14</sup> Ellen Nakashima, “White House Says Sony Hack Is A Serious National Security Matter,” *Washington Post*, December 18, 2014, [https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25\\_story.html?noredirect=on&utm\\_term=.263af0131909](https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25_story.html?noredirect=on&utm_term=.263af0131909).

coordinate cyberspace planning and operations.<sup>15</sup> The broad questions associated with how cyber fits within the constructs of international laws have been continually discussed within government, the private sector, and academic circles. Nations agree that these laws should apply to the cyber domain, but the question remains: *how*?

During the Atlantic Council's April 2019 Eighth Annual International Conference on Cyber Engagement (ICCE) in Washington, DC, a group of experts discussed multidisciplinary approaches to develop international collaboration and norms to act against growing cyberattacks.<sup>16</sup> David Koh, chief executive of Singapore's Cyber Security Agency, advised of the need for a whole-of-government global engagement to develop a legal framework of measures and oversight: a "vibrant cybersecurity ecosystem."<sup>17</sup> The borderless cyber environment requires a mutual effort to establish a rules-based cyberspace, similar to the UN Conventions on the Law of the Sea: a pivotal work that extended international law to the vast, 140 million square miles of ocean; established freedom-of-navigation rights; and created territorial sea boundaries, exclusive economic zones, and rules for extending continental shelf rights.<sup>18</sup> International order is necessary for the collective security of all nation-states. The question is *how* does the international community effectively develop, fully adapt, and implement order within the cyber domain?

Is it possible to govern a space that does not have tangible borders? This question has been explored and discussed throughout the international cyber community as activities—both innocent and nefarious—increase within the cybersphere. The international community concurs that international laws should apply to the cyber domain; the disagreements lie in *how* they should apply. The majority of research and discussions have focused on the application of international laws to state actors. This thesis takes it a

---

<sup>15</sup> "About History," U.S. Cyber Command, accessed May 10, 2019, <https://www.cybercom.mil/About/History/>.

<sup>16</sup> Catherine Lotrionte, "Atlantic Council Eighth Annual International Conference on Cyber Engagement (ICCE): Introductory Remarks" (symposium, G.W. Lisner Auditorium, George Washington University, Washington, DC, April 22, 2019), <https://www.atlanticcouncil.org/icce>.

<sup>17</sup> David Koh, "Atlantic Council Eighth Annual International Conference on Cyber Engagement (ICCE): Keynote Address" (symposium, G.W. Lisner Auditorium, George Washington University, Washington, DC, April 22, 2019), <https://www.atlanticcouncil.org/icce>.

<sup>18</sup> Koh.

step further, exploring the question: How could international laws apply to non-state actors within the cyber domain during peace-time operations?

## **B. RESEARCH QUESTION**

Is the NATO CCDCOE, using the Budapest Convention framework, the correct regulatory entity for international governance of non-state actors in the cyber domain? Is one governing entity sufficient or should there be a multipronged approach for dispute resolution?

## **C. LITERATURE REVIEW**

A literature review on the application of international norms and law, including the Laws of War, *jus ad bellum* (law concerning use of force during war) and *jus in bello* (law concerning conduct during war), yields three main categories: existing international law and the Laws of War as they apply to the cyber domain, development of an entirely new and unique set of rules on cyberspace, and the establishment of a central international governing body to mitigate disputes.

Sanctity exists within international law, as Madeleine Albright once revealed: it is a “body of norms made by states for states, and its content and application are almost always open to honest dispute.”<sup>19</sup> An issue with international law, which will be encountered as the world tries to govern non-state and proxy state actors, is the lack of one power or governing body with the ultimate authority to interpret international law for everyone.<sup>20</sup> Currently, each state has the right and obligation to interpret international law for itself.

In 2011, the UN “Group of Governmental Experts” on cyber issues noted the “U.S. acceptance of the applicability of the [Laws of War]—*jus ad bellum* and *jus in bello*—to

---

<sup>19</sup> Lee Casey and David B. Rivkin, *International Law and the Nation-State at the U.N.: A Guide for U.S. Policymakers*, Heritage Foundation, August 18, 2016, 2. <https://www.heritage.org/global-politics/report/international-law-and-the-nation-state-the-un-guide-for-us-policymakers>.

<sup>20</sup> Casey and Rivkin.

activities in cyberspace.”<sup>21</sup> This document furthered discussions of conventional legal applicability to the cyber domain but left open the question as to *how* these Laws of War and international laws should apply in the cyber domain, *by which authority* they should be governed, and *what extra regulatory measures*, if any, need to be emplaced.

The cyber domain remains an area of uncertainty with regard to international regulation. U.S. Department of State Legal Advisor Harold Koh explained in his address to the 2012 U.S. Cyber Command (USCYBERCOM) Inter-Agency Legal Conference that international law applies to the cyber domain and identified several unresolved future issues in cyberspace, such as the possible need to develop unique regulations.<sup>22</sup> In his 2018 thesis, Ike Barnes proposed NATO’s CCDCOE, which facilitated the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn 2.0)*, as an international governance framework to mitigate cyber disputes.<sup>23</sup> Global engagements, including the 2001 Budapest Convention on Cybercrime, have furthered discussions on the need for international governance; however, a consensus has not been reached as to composition or limitations of such a governing institution.<sup>24</sup>

Establishing attribution is a critical step in cyber operations, one that is neither simple nor automated. Attribution is one of the challenges in determining whether an actor is a state, non-state, or a proxy state actor. Reviewing existing or proposed attribution processes remains outside the scope of this thesis. It will only be mentioned in context of a proposed international governance process once the cyber action is attributed based on cyber community attribution indicators such as tradecraft, infrastructure, malware, intent,

---

<sup>21</sup> “Developments in the Field of Information and Telecommunications in the Context of International Security,” United Nations Office for Disarmament Affairs, 2011, <https://www.un.org/disarmament/ict-security/>.

<sup>22</sup> Harold Honhgu Koh, “International Law in Cyberspace” (conference, USCYBERCOM Inter-Agency Legal Conference, Ft. Mead, MD, Sept. 18, 2012) <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>.

<sup>23</sup> Isaac A. Barnes, “Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International Body to Address Disputes” (master’s thesis, Naval Postgraduate School, 2018), [https://calhoun.nps.edu/bitstream/handle/10945/61274/18Dec\\_Barnes\\_Isaac.pdf?sequence=1&isAllowed=y](https://calhoun.nps.edu/bitstream/handle/10945/61274/18Dec_Barnes_Isaac.pdf?sequence=1&isAllowed=y).

<sup>24</sup> Elena Chernenko, Oleg Demidov, and Fyodor Lukyanov. “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms,” Council on Foreign Relations, February 23, 2018, <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms>.

and external source reporting.<sup>25</sup> To effectively govern cyber activities and possibly levy sanctions or other remedies, the action needs to be attributed to the appropriate party or parties for proper routing within the governance process. Cyber activities by non-state actors have been multiplying over the last decade, thus driving the transformation of international debates and relationships. However, the U.S. National Intelligence Council in 2007 warned that very few standalone non-state actors exist; most are dependent upon—in some manner—nation-states and lack autonomous latitude.<sup>26</sup> Pure, independent non-state freedom of movement is greater in weak or post-industrial states than in modernized states such as Russia and China, where the governments suppress independent actors and have their own powerful cyber entities capable of influencing global powers such as the United States. When determining attribution for the purpose of the international governance process, a key component will be factors that denote a non-state actor's relationship to a nation-state, a distinguishing factor in the remedies stage.

Another factor in determining culpability of non-state actors will be benign or non-benign branding. Several variations of the “non-state actor” definition abound, but without consensus as to the composition of the category and who should or should not be branded. For instance, trade unions, religious organizations, communities, and academic institutions are sometimes included in the classification. The National Intelligence Council defines non-state actors as “non-sovereign entities that exercise significant economic, political, or social power and influence at a national, and in some cases international, level.”<sup>27</sup> Benign non-state actors, such as most multi-national corporations, nongovernmental organizations (NGO), or highly-influential philanthropic individuals pose minimal threat to U.S. and international security. Due to the minimal threat, they are often overlooked in geopolitical discussions and will only be mentioned in this thesis for defining non-state actor categories. The specific non-state actors discussed in this thesis are the benign, truly non-state

---

<sup>25</sup> “A Guide to Cyber Attribution,” Office of the Director of National Intelligence, 3, September 14, 2018. [https://www.dni.gov/files/CTIIC/documents/ODNI\\_A\\_Guide\\_to\\_Cyber\\_Attribution.pdf](https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf).

<sup>26</sup> “Nonstate Actors: Impact on International Relations and Implications for the United States,” National Intelligence Council, 1, 2007. [https://www.dni.gov/files/documents/nonstate\\_actors\\_2007.pdf](https://www.dni.gov/files/documents/nonstate_actors_2007.pdf)

<sup>27</sup> National Intelligence Council, 2.

individuals and organizations with functions completely independent from national governments and nation-state entities.

As the cyber domain continues to rapidly expand, so too will the cyber threats against the United States and international partners. The literature supports the notion that nation-states, notably China, Russia, North Korea, and Iran, as well as malign non-state actors and proxies, increasingly use cyber as low-cost method for conducting transnational, global operations to advance their interests.<sup>28</sup> It is imperative to continue driving the international governance discussion to formulate transnational preparedness, mitigation and response to a growing and potentially escalating cyber environment. In 2004, the United Nations (UN) recognized the need for a paradigm shift not only from an intergovernmental body to including civil society (non-state groups) engagement, but also stressed the importance of non-state actors in the global ecosystem, with the recommendation that the UN take a proactive approach in “bringing together all constituencies relevant to global issues, and galvanizing appropriate networks for effective results.”<sup>29</sup> Prioritizing the cyber governance discussion with proposed responsibilities and roles, in whole or in part, for international organizations such as the UN advances this proactive approach.

A main part of this thesis arose from a 2018 Center for Homeland Defense and Security (CHDS) thesis by Isaac “Ike” Barnes. It focused on the Active Cyber Defense Certainty (ACDC) Act, Cyber Diplomacy Act of 2017 (CDA), and the need to couple them along with the creation of a national Director of Cybersecurity position, similar to the Director of National Intelligence, to effectively transform the current passive cybersecurity posture to one focused on active defense. The ACDC Act, nicknamed the “Hack Back Bill,” is bipartisan U.S. legislation (H.R. 4036) proposed on October 13, 2017, to amend

---

<sup>28</sup> Daniel R. Coats, “Worldwide Threat Assessment of the U.S. Intelligence Community,” Office of the Director of National Intelligence, January 29, 2019, <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>; Koh, “International Law in Cyberspace;” National Intelligence Council, “Nonstate Actors”; Chernenko, Demidov, and Lukyanov, “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms.”

<sup>29</sup> “United Nations Urged to Pay More Heed to Role of ‘Non-State Actors’ in Approach to Global Problems,” United Nations, June 21, 2004, <https://www.un.org/press/en/2004/sg2089.doc.htm>.

the Computer Fraud and Abuse Act by limiting negative consequences for parties that engage in counterattack or defense measures to cyber intrusions, also dubbed “active defense.”<sup>30</sup> The last action on the ACDC Act was on November 1, 2017, when it was referred by the Congressional Committee on the Judiciary to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. The CDA was introduced in September 2017 (H.R. 3776), passed the House and passed to the Senate as CDA of 2018 in June 2018. The bill proposed cyber policy promoting “an open, interoperable, reliable, unfettered, and secure Internet governed by a model that promotes human rights, democracy, and the rule of law, while respecting privacy and guarding against deception, fraud, and theft.”<sup>31</sup> It also called for establishment of a Department of State Office of Cyber Issues, and encouraged the president of the United States to “enter into executive arrangements with foreign governments that support the cyberspace policy.”<sup>32</sup> The CDA of 2019 (H.R. 739) expanded on CDA of 2018 to establish a Department of State Office of International Cyberspace Policy to implement the U.S. international cyber policy mentioned in CDA of 2018, serve as an advisor for cyber issues, lead cybersecurity diplomatic efforts, and direct the president to “devise a strategy related to U.S. engagement with foreign governments on international norms with respect to responsible state behavior in cyberspace.”<sup>33</sup> The bill has been sitting with the House Committee on Foreign Affairs for consideration since March 2019. Barnes’ approach considers the CDA a mechanism for U.S. companies’ behavior in cyberspace, supporting the use of active cyber defense.

Rounding out this holistic approach, Barnes discussed the need for a dispute-mitigation entity. He identified the NATO CCDCOE together with the Budapest Convention on Cybercrime to provide a framework and dispute resolution entity. Barnes’s designation of the CCDCOE as a governing body is based on Centre’s history with

---

<sup>30</sup> Active Cyber Defense Certainty Act, H.R. 4036, 115th Congress (2017-2018) <https://www.congress.gov/bill/115th-congress/house-bill/4036/text>.

<sup>31</sup> Cyber Diplomacy Act of 2018, H.R. 3776, 115th Congress, <https://www.congress.gov/bill/115th-congress/house-bill/3776>.

<sup>32</sup> Cyber Diplomacy Act of 2018.

<sup>33</sup> Cyber Diplomacy Act of 2019, H.R.739, 116th Congress, <https://www.congress.gov/bill/116th-congress/house-bill/739>.

cybersecurity: specifically, its international group of experts (IGE) who interpreted and restated international law as applied to the cyber domain. These restatements—black letter rules—are contained within *Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn)* and *Tallinn 2.0*. Barnes’s argument is that by empowering the CCDCOE to mitigate cyber disputes, information-sharing will be easier while at the same time making it harder for “enemies to remain anonymous.”<sup>34</sup> In addition to stating that the U.S. Executive Branch should work with international partners to determine the best active cyber defense measures in accordance with the ACDC Act, he states the Executive Branch also has an integral role in modifying the NATO charter to enable and allow for the CCDCOE to continue its *Tallinn 2.0* legal analysis and to develop into a governance body responsible for dispute mitigation and resolution.<sup>35</sup>

This thesis leverages the following future areas of study that Barnes recommended, taking them a step further to focus on purely non-state actors:

- What is the process flow between nations to resolve disputes pertaining to non-state actors?
- “How will the CCDCOE resolve the inevitable disputes” regarding non-state actors/malign acts?
- “What is the mechanism to bring the disputes before the CCDCOE?”
- Is the CCDCOE the correct entity for disputes? If not, what are other options? Is it a singular body or a network of governing bodies to effectively regulate the cyberspace pertaining to non-state actors?
- Develop procedures to employ recommendations from his thesis and this research.

---

<sup>34</sup> Barnes, “Implementation of Active Cyber Defense Measures by Private Entities,” 57.

<sup>35</sup> Barnes, 53.

#### **D. RESEARCH DESIGN**

This thesis discusses the current cyber landscape and examines existing international law and regulatory mechanisms as they apply to the cyber domain, generally, and to non-state actors, specifically. The thesis examined several of Barnes's future course of study in the context of non-state cyber activities. Based on concurrence or disapproval of his suggestions, it offers alternative solutions for regulatory mechanisms or processes. Likewise, it recommends future areas of study to explore additional remedies, including sanctions and other regulatory measures, if any, that may need to be created to address areas not covered by existing laws. Subject matter analysis from multiple datasets provided insight into the existence, enforcement, and effectiveness of international law application to the cyber domain, as well as missing pieces in cyber international governance. This research examined cyber rules of engagement (ROE), restatement of international law as they pertain to the cyber domain, frameworks, and international bodies with cyber influence.

Once it was understood how international laws could be applied to the cyber domain, the next step examined the types of processes that could be developed to regulate non-state actors as well as how they could be applied and by what body or bodies. This research focused attention on Barnes's proposed framework, the Budapest Convention, and NATO's CCDCOE as well as alternative options for the composition and location of a dispute resolution solution. The research studied the pros and cons of a possible single solution governance or a combination of entities through a multi-pronged approach. The solutions are identified, examined, and assessed through gap and process analyses based on binary adaptability within existing legal frameworks, authorities, governance, and enforcement challenges to determine current status, deficiencies, and actions required to move forward and remedy the deficiencies.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. CYBER THREATS AND POLICY RESPONSES**

This chapter provides the reader with an understanding of the current layout of cyberspace. First, it reflects on the current power competition between the key players in today's cyberspace—China, Russia, North Korea, and the United States. Next, the chapter lays out significant policy developments that helped shape the United States response to its main adversaries. Finally, it paints a picture of the three main categories of actors—state, non-state, and proxy state actors—in the cyber domain, discussing each role with examples. Although the thesis focuses on non-state actors, it is essential to have a holistic picture and situational awareness of the problem area to understand the key players and their roles in cyberspace.

### **A. POWER COMPETITION WITH CHINA, RUSSIA AND NORTH KOREA**

The 2018 Department of Defense (DOD) *Cyber Strategy* acknowledges that the United States is engaged in long-term strategic cyber competition with Russia and China as well as facing continuous malicious cyber threats from North Korea that pose serious risks to our nation as well as our allies and partners.<sup>36</sup> The strategy stresses the importance of defending forward—taking preemptive, active rather than reactive, assertive operations to degrade adversarial cyber activities as close to the source as possible before reaching U.S. assets, building a skilled cyber force, securing critical information systems and infrastructure, and engaging with partners to protect against malicious cyber activity.

#### **1. China**

China's sophisticated technological capability and power drive gives the country an advantage as one of the top major threats in the cyber domain. President Xi Jinping has stated his desires to turn China in a "cyber-superpower," and it has been ramping up its

---

<sup>36</sup> Department of Defense, *Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), 3, [https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).

efforts to achieve this goal.<sup>37</sup> With a newly established Cyberspace Administration of China and four cyber-focused national priorities, China and the People's Liberation Army (PLA) are determined to increase their cyber forces and network defenses while also closing off external access ("cyber-sovereignty"). In addition to its offensive capability, China has a defensive advantage through its "Great Firewall—the digital equivalent of their [physical] Great Wall—designed to require external communications to pass through several official filters.<sup>38</sup> China's research and development has grown 20 percent a year since 1999 and is estimated at US\$233B; in addition, its quantum computing advances could enable China intelligence to create and break U.S. encryption channels.<sup>39</sup> China's increasing political control over its technology sector, which supplies digital infrastructure worldwide, opens up the opportunity for Chinese cyber-espionage. Eight companies are in China's domestic supply chain in what the country coins, the "8 King Kongs": Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm.<sup>40</sup> China's reliance on these companies for its internet technology infrastructure project a mission that is defensive, rather than offensive. However, in December 2015 the Chinese established the PLA Strategic Support Force "probably to improve oversight and command of Beijing's growing military interests in space and cyberspace."<sup>41</sup> The creation of this cyberspace and electronic warfare branch for military support and reform gives the perception, at the very least, that China is taking a preemptive, offensive stance rather than reducing aggression.

In a recent CBS News interview, Secretary of State Michael Pompeo recently stated that "the theft of American intellectual property is a big business [for China] to the tune of hundreds of billions of dollars and President Trump is determined to push back against

---

<sup>37</sup> Adam Segal, "When China Rules the Web: Technology in Service of the State," *Foreign Affairs*, September 2018, <https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web>.

<sup>38</sup> Geremie R. Barme and Sang Ye, "The Great Firewall of China," *Wired*, June 1 1997, <https://www.wired.com/1997/06/china-3>.

<sup>39</sup> Segal, "When China Rules the Web."

<sup>40</sup> Jinghua Lyu, "What Are China's Cyber Capabilities and Intentions?" IPI Global Observatory, April 1, 2019, <https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734>.

<sup>41</sup> Patrick Howell O'Neill, "DNI: Chinese Hacking Against U.S. Companies Is 'Ongoing' But 'Significantly Reduced,'" *Cyberscoop*, May 23, 2017, <https://www.cyberscoop.com/china-us-hacking-odni-dan-coats-2017/>.

it.”<sup>42</sup> FBI Director Christopher Wray also stated that “No country poses a broader threat ... than China” whose long-term cyber strategies are calculated and persistent.<sup>43</sup> While much attention the last couple years has been focused on Russia’s cyber activities and meddling, North Korea and China have been increasing their activities with an “uptick of blended threats in which foreign governments join forces with cyber criminals.”<sup>44</sup> The depth and breadth of China’s activities, combined with our system vulnerabilities, pose a greater cyber threat to homeland security than solely the Russia problem.

## 2. Russia

Russia is a dominating power within the cyber domain. The Kremlin uses cyber espionage and malicious cyberattacks to project power, influence communications, interfere in nation-state government affairs, and establish traction in organizations. Russian cyber activities trend toward “weaponization” of information—manipulating social and news media to influence public opinion and undermine credible sources.<sup>45</sup> A prime example of Russian information weaponization was their misinformation campaign targeting American voters during the 2016 U.S. presidential election. The Kremlin utilized Facebook trolls to post inflammatory messages and elicit emotional responses that steered election candidate discussions in certain directions.<sup>46</sup> In addition, the Russians ran unregulated, divisive political ads on Facebook to further influence the elections.<sup>47</sup>

---

<sup>42</sup> Erin Banco, “FBI Director Christopher Wray Says Russia Remains a Threat to the 2020 Election,” *Daily Beast*, April 26, 2019, <https://www.thedailybeast.com/fbi-director-christopher-wray-says-russia-remains-a-threat-to-2020-election>.

<sup>43</sup> Banco.

<sup>44</sup> Teri Robinson, “FBI Director Wray Says Cyber-threats ‘Bigger Than Government,’” *SC Magazine*, March 7, 2019, <https://www.scmagazineuk.com/fbi-director-wray-says-cyber-threats-bigger-government/article/.1578178>.

<sup>45</sup> Ed Parsons and Michael Raff, “Understanding the Cyber Threat from Russia,” F-Secure, accessed March 22, 2020, <https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-russia>.

<sup>46</sup> Issie Lapowsky, “How Russian Facebook Ads Divided and Targeted U.S. Voters Before the 2016 Election,” *Wired*, April 16, 2018, <https://www.wired.com/story/russian-facebook-ads-targeted-us-voters-before-2016-election/>.

<sup>47</sup> Lapowsky.

Russia's meddling and misinformation campaign helped swing the U.S. presidential election away from Hillary Clinton in favor of Donald Trump.

Russian-backed cyberattacks have increased in frequency and destructiveness. In October 2017, President Trump signed a law that banned Moscow-based anti-virus firm Kaspersky Lab within the U.S. government. The concern was that the firm had ties to the Russian government, posing a grave risk to national security via cyber espionage.<sup>48</sup> Russia's cyber policy has transitioned from information-gathering to offensive disruptions. During the 2018 Olympics Games in Pyeongchang, South Korea, the International Olympic Committee suspended and prohibited 168 Russian athletes from competing under the Russian flag based on doping evidence.<sup>49</sup> In retaliation, the Russian government attacked the games' opening ceremony, shutting down Seoul data servers, the backbone of the Olympics' IT infrastructure.<sup>50</sup> The Russian hackers used their trademark deception technique: creating layers of false flags to direct attribution elsewhere, in this case, toward North Korea.<sup>51</sup> Only after in-depth, painstaking forensic analysis and examination of hidden connections and cyber fingerprints was the attack attributed to the Kremlin.

The 2018 Pyeongchang Olympics and the 2016 U.S. election misinformation campaign demonstrate Russia's advancement in deception techniques and sophisticated malicious cyber campaigns.

### **3. North Korea**

In its 2019 global cyber threat report, CrowdStrike, a cybersecurity firm, described North Korea as a growing threat with its Democratic People's Republic of Korea (DPRK)-

---

<sup>48</sup> Dustin Volz, "Trump Signs Into Law U.S. Government Ban on Kaspersky Lab Software," December 12, 2017, Reuters, <https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4>.

<sup>49</sup> Elias Chakhak, "Winter Olympics Cyber Attack Signs Point to Russia—So Why the False-Flag?" Cyber Research Databank, accessed March 22, 2020, <https://www.cyberdb.co/winter-olympics-cyber-attack-all-signs-point-to-russia/>.

<sup>50</sup> Joan Wong, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," *Wired*, October 17, 2019, <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>.

<sup>51</sup> Wong.

based malicious activity—Hidden Cobra—supporting two primary areas of interest: financial targeting (currency generation efforts for Kim Jong-Un) and acquiring diplomatic information related to the U.S. and South Korea policy decisions.<sup>52</sup> CrowdStrike has dubbed four hacking subgroups of North Korea’s notorious Lazarus group—Stardust Chollima, Silent Chollima, Labyrinth Chollima, and Ricochet Chollima—that appear to be launching attacks on behalf of the government, from cryptocurrency spear-phishing campaigns to supporting cyberespionage efforts.<sup>53</sup> While the U.S. Congress was focused on fake Russian Facebook profiles during the 2016 election, nothing was publicized about North Korea’s fake profile campaigns (e.g., the Lazarus Group created its own fake copy of a Korean bible reading Android [malware] app to target South Koreans, which was widely available on Google Play).<sup>54</sup>

North Korea is especially dangerous because of Kim Jong Un’s unpredictability. Forecasters believe that rising tensions between the United States and North Korea will, based on previous attacks, set in motion increased cyberattacks. Geopolitical tension surrounding the North Korean nuclear program are likely to precipitate North Korean–state-sponsored malicious cyber activity against South Korea, Japan, and the United States. In its February 2019 report, “The Evolution of North Korean Cyber Threats,” the Asan Institute for Policy Studies came to similar conclusions based on North Korea’s 7,000-hacker-strong cyber “army” and that low-cost, low-risk cyber operations allow the country to attack with little fear of retaliation.<sup>55</sup>

---

<sup>52</sup> “2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed,” CrowdStrike, accessed January 3, 2020, [https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gtr?utm\\_campaign=Threat\\_Report\\_2019&utm\\_medium=Web&utm\\_source=Marketo](https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gtr?utm_campaign=Threat_Report_2019&utm_medium=Web&utm_source=Marketo).

<sup>53</sup> “Hidden Cobra—North Korean Malicious Cyber Activity,” Cybersecurity and Infrastructure Security Agency, accessed 8/3/2019, <https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity>.

<sup>54</sup> CrowdStrike, “2019 Global Threat Report.”

<sup>55</sup> Kim Chong Woo, “The Evolution of North Korean Cyber Threats,” Asan Institute, February 20, 2019, <http://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/>.

## **B. U.S. CYBER POLICY DEVELOPMENTS**

Cyberspace is a focal point for U.S. and international interests, linking military, social, political, and economic power applications for modern life. Key policy developments have shaped U.S. cyber activities over the years. In-depth research and analysis could provide insight to the complexities of each policy and the national position as it evolves. An overview of cyber policy history provides a holistic framework for understanding of the current state of U.S. cyber policy.

Interdependence of battlespace domains and their reliance on cyber technology stresses the need for offense-based cyber policy implementation.<sup>56</sup> Employment of a “more agile and expansive approach” will incorporate cyber operations as a tool in counterterrorism efforts to stay ahead of our adversaries who pose a threat to the homeland.<sup>57</sup> Several existing authorities will facilitate forward movement toward offense-based policy implementation. The National Security Act of 1947, created following World War II, restructured U.S. military and intelligence agencies and established the DOD, Secretary of Defense, National Security Council, CIA, NSA, and other agencies.<sup>58</sup> The act established an official process for national security decisions and intelligence oversight.<sup>59</sup> Titles 10 and 50 of the U.S. Code are mutually supporting authorities for leading U.S. offense-based cyber operations. Title 50 governs U.S. military and intelligence operations, to include cyberspace, in defense of the United States.<sup>60</sup> Executive Order 12333 has regulated the IC since 1981, but also directs the Secretary of Defense to “collect (including through clandestine means), analyze, produce, and disseminate information and intelligence [as well as] ... defense and defense-related

---

<sup>56</sup> Joint Chiefs of Staff, *Cross-Domain Synergy in Joint Operations: Planner’s Guide*, 51. (Washington, DC: Joint Chiefs of Staff, 2016.) [http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross\\_domain\\_planning\\_guide.pdf?ver=2017-12-28-161956-230](http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230).

<sup>57</sup> White House, *The National Strategy for Counterterrorism* (Washington, DC: White House, 2018), 2, <https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf>.

<sup>58</sup> Department of State, Office of the Historian. “National Security Act of 1947,” accessed November 20, 2018, <https://history.state.gov/milestones/1945-1952/national-security-act>.

<sup>59</sup> National Security Act of 1947, Public Law No. 235, 61 Stat. 496 (1947).

<sup>60</sup> War and National Defense, *U.S. Code* 50 §§ 1–2420, accessed November 21, 2018, <https://www.law.cornell.edu/uscode/text/50>.

intelligence and counterintelligence.”<sup>61</sup> Thus, military intelligence authorities provide a baseline for offense cyber-related operations and support.

Title 10 also created combatant commands with statutory authorities whose commanders report directly to the Secretary of Defense. USCYBERCOM was officially created on November 12, 2008, under then-Defense Secretary Gates as a sub-unified command under U.S. Strategic Command, attaining initial operating capability on May 21, 2010. At the time, USCYBERCOM was codified under a “dual-hat” authority with the NSA.<sup>62</sup> The USCYBERCOM mission is to “direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.”<sup>63</sup> USCYBERCOM is located in Fort Meade, Maryland, and executes its cyber mission through four sub-unified military service cyber units:

- 2nd Army—U.S. Army Cyber Command
- 24th Air Force—Air Force Cyber
- U.S. Tenth Fleet—Fleet Cyber Command
- U.S. Marine Corps Forces Cyberspace Command<sup>64</sup>

Each of these units directs “cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters DOD’s cyber expertise.”<sup>65</sup> USCYBERCOM’s structure is intended to design and train the cyber force, coordinate with international and interagency partners, and assure seamless mission execution. It is too soon in the U.S.

---

<sup>61</sup> Ronald Reagan, Executive Order 12333, “United States Intelligence Activities,” *Code of Federal Regulations*, title 3 (1981), <https://www.cia.gov/about-cia/eo12333.html>. accessed November 21, 2018.

<sup>62</sup> U.S. Cyber Command. “About History.”

<sup>63</sup> U.S. Cyber Command. “About Mission and Vision.” accessed October 1, 2018. <https://www.cybercom.mil/About/Mission-and-Vision/>.

<sup>64</sup> U.S. Cyber Command. “About History.”

<sup>65</sup> U.S. Cyber Command. “About Mission and Vision.”

cyberspace effort to conclude if the process is working or if it presents a fragmented approach that calls for restructuring of the command.

The 2008 National Security Presidential Directive (NSPD-54) and Homeland Security Presidential Directive (HSPD-23) launched the Comprehensive National Cybersecurity Initiative (CNCI). The initiative was released by George W. Bush and outlines U.S. cybersecurity policy, organizational, and security goals across the federal government. The CNCI was an effort to coordinate cyber policy across public and private sectors. Upon its public release on June 5, 2014, the unclassified version provided the public with new insight into U.S. cybersecurity, offense-based programs, tools, and policy efforts.<sup>66</sup> These efforts assured the public that the United States was fully stepping into cyberspace to develop its power in the newest battlespace domain.

One of the Obama administration's objectives was to develop the CNCI into key elements of the broader national cybersecurity strategy and Obama's Cyberspace Policy Review.<sup>67</sup> In 2011, President Obama implemented the *International Strategy for Cyberspace*, which stated the U.S. goal to internationally "promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation" through development of rules of conduct within the laws governing cyberspace.<sup>68</sup> This strategy was intended to be a roadmap for better coordination of roles, definitions, and implementation of cyber policy. Ambiguity still exists regarding rules of conduct and governing cyberspace laws, which is discussed in the following text. The United States should be committed to leading dialogue, sharing best practices, and building relationships on critical cyber issues. President Obama signed Presidential Policy Directive (PPD-20) *U.S. Cyber Operations Policy* in 2012, which superseded the Bush

---

<sup>66</sup> "EPIC v. NSA: NSPD-54 Appeal Freedom of Information Act," EPIC, accessed November 18, 2018, <https://epic.org/foia/nsa/nspd-54/appeal/>.

<sup>67</sup> "Preventing and Defending Against Cyber Attacks," Department of Homeland Security, 2011. <https://www.dhs.gov/news/2011/10/18/preventing-and-defending-against-cyber-attacks>

<sup>68</sup> White House, *The, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, 2011). [https://obamawhitehouse.archives.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

Administration's NSPD-38, *National Strategy to Secure Cyberspace*, and complemented NSPD-54 and HSPD-23 by integrating cyber tools with national security. The directive required an oversight review process from the U.S. Department of State and IC agencies before the military could launch an offense-based cyberattack, which could be viewed as cumbersome and time consuming. Critics have argued that the PPD-20 involves too many agencies that hinder and slow down potential cyber planning.<sup>69</sup> Others deemed the review process necessary to ensure civilian control over the military, prevent unnecessary escalation, promote fair decision-making, and avoid overlap with existing operations.<sup>70</sup>

In 2011, private U.S. cybersecurity firms began highlighting the damage caused by rampant Chinese hackers.<sup>71</sup> The United States is a continual espionage target of China, which uses hackers and spies to obtain U.S. trade, patent, and military information, allowing Chinese companies access to U.S. technology Research and Development “details of countless pieces of American military hardware, from fighter jets to ground vehicles.”<sup>72</sup> In 2013, President Barack Obama raised the issue of cyber-hacking, debating deterrent and punitive options but was met with pushback from inside his administration.<sup>73</sup> In 2014, the United States finally achieved some leverage over China when it indicted five PLA members for cyberespionage—the first time the United States indicted state-sponsored actors for a cybercrime.<sup>74</sup> The PLA ran China's main cyber campaign for almost 10 years between 2005 and 2014; however, once PLA members were detained by the United States, the Chinese Ministry of State Security became the preeminent driver of a powerful cyber

---

<sup>69</sup> Adam Raymond, “Trump Makes It Easier for the Military to Launch Cyberattacks,” *New York Magazine*, August 16, 2018, <http://nymag.com/intelligencer/2018/08/trump-makes-it-easier-for-the-u-s-to-launch-cyber-attacks.html?gtm=top&gtm=bottom>.

<sup>70</sup> Mach DeGeurin, “U.S. Silently Enters New Age of Cyberwarfare,” *New York Magazine*, September 2018, <http://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html>.

<sup>71</sup> Garret Graff, “How the U.S. Forced China to Quit Stealing—Using a Chinese Spy,” *Wired*, October 11, 2018, <https://wired.com/story/us-china-cybertheft-su-bin>.

<sup>72</sup> Graff.

<sup>73</sup> Greg Miller, Ellen Nakashima, and Adam Entous, “Obama's Secret Struggle to Punish Russia for Putin's Election Assault,” *Washington Post*, June 23, 2017, [https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm\\_term=.3ecae726ee00](https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.3ecae726ee00).

<sup>74</sup> “Indictment of PLA Officers,” Council on Foreign Relations, May 2014, <https://www.cfr.org/interactive/cyber-operations/indictment-pla-officers>.

espionage campaign against the United States.<sup>75</sup> The continuing Chinese threat cemented a requirement for domestic and international cyber regulatory mechanisms for cyber disputes.

The PLA confrontation was a broader effort to define cyberspace norms. In 2015, President Barack Obama and President Xi Jinping entered the United States and China into a bilateral Cyber Agreement to reduce aggression and instability in cyberspace, including known cyber-related intellectual property theft and joint cybercrime dialogue, and promoting “appropriate norms of state behavior in cyberspace within the international community.”<sup>76</sup> The cyber discussions that led to the agreement arose out of a history of persistent Chinese government cyberattacks against the U.S. government. Of particular note, President Barack Obama vowed to countervail to attract China’s attention in response to PLA indictment.<sup>77</sup> After the first few months of the agreement, there was a significant reduction in cyber espionage attacks attributed to the Chinese.<sup>78</sup> However, China continues to develop its cyber strategy in response to the evolving cyber domain as well as to align with its military and national security strategies.

In April 2015, the DOD released *Cyber Strategy*, which contained five strategic goals that included relationship building, defensive security, and managing conflict escalation. to the strategy strengthens U.S. cyber deterrence and aligns with DOD’s three cyber missions to “defend DOD networks, systems, and information; defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and support operational and contingency plans.”<sup>79</sup> See Figure 2 for a recent depiction of the DOD *Cyber Strategy* aligned with its other strategies, including national security.

---

<sup>75</sup> Graff, “How the U.S. Forced China to Quit Stealing.”

<sup>76</sup> John W. Rollins, “U.S.-China Cyber Agreement,” *Congressional Research Service*, October 16, 2015. <http://www.fas.org/sgp/crs/index.html>.

<sup>77</sup> Rollins.

<sup>78</sup> O’Neill, “DNI.”

<sup>79</sup> Department of Defense, *The DoD Cyber Strategy* (Washington, DC: Department of Defense, 2015), [http://archive.defense.gov/home/features/2015/0415\\_cyber-strategy/final\\_2015\\_dod\\_cyber\\_strategy\\_for\\_web.pdf](http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf).

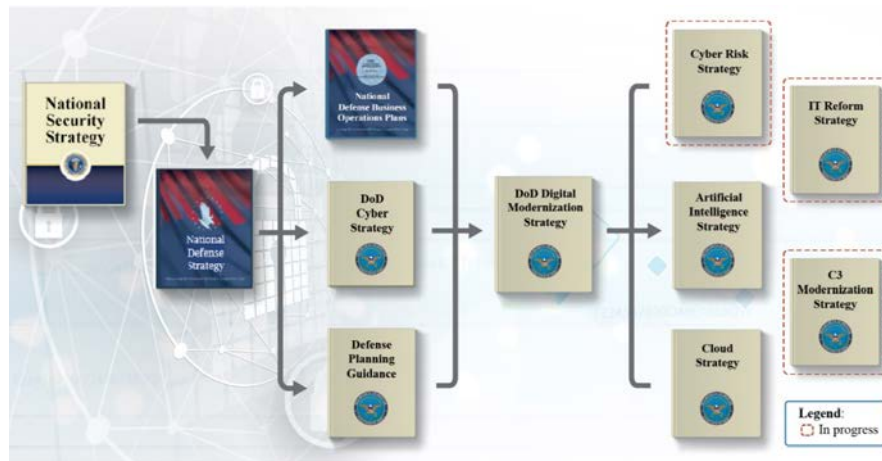


Figure 2. DOD Cyber Strategy Alignment with DOD Guidance<sup>80</sup>

The first strategic goal, to “build and maintain ready forces and capabilities to conduct cyberspace operations” to be properly equipped for effective operation in cyberspace, is the foundation for implementing U.S. cyber policy and developing a powerful cyberspace presence.<sup>81</sup>

An assertive offense-based cyber strategy may not be the most favorable method for U.S. leadership, diplomats, and top private-sector executives who may be more concerned about sensitive bilateral strategic relationships than data and intellectual property stolen or affected by cyberhackers. Diplomacy is the heart of international partner relationships, providing foreign country representatives with an understanding of U.S. perspectives on foreign policy issues and facilitates important, often complex, bilateral and multilateral agreement negotiations for treaties, accords, conventions, and alliances.<sup>82</sup> Jeopardizing diplomatic ties could cause political entities to shy away from offense-based support.<sup>83</sup>

<sup>80</sup> Source: Department of Defense, *DoD Digital Modernization Strategy 2019* (Washington, DC: Department of Defense, 2019), <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DoD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>.

<sup>81</sup> Department of Defense, *The DoD Cyber Strategy*, 13.

<sup>82</sup> “Diplomacy 101.” Department of State, accessed October 5, 2018. <https://www.state.gov/discoverdiplomacy/diplomacy101/issues/170614.htm>.

<sup>83</sup> Graff, “How the U.S. Forced China to Quit Stealing.”

The State Department is the U.S. leader in diplomatic engagement to achieve foreign policy objectives.<sup>84</sup> The department submitted to Congress its International Cyberspace Strategy in April 2016, reflecting three themes to support the President’s International Strategy for Cyberspace (released in 2011): the applicability of international law; the importance of promoting confidence building measures; and the significant progress the department has made, working in partnership with other federal departments and agencies, to promote international norms of state behavior in cyberspace, as well as future plans in this area.<sup>85</sup> The document focused mostly on U.S.–China cyber commitments, “diplomatic efforts to shape the policy environment, building a framework for international stability in cyberspace,” and tools available to deter malicious actors.<sup>86</sup> The State Department strategy champions a multi-stakeholder approach to internet governance utilizing whole-of-government tools to achieve its objectives.<sup>87</sup> However, the document fails to state how, exactly, the tools will be used or what roles the stakeholders would play.

The 2017 National Security Strategy introduced a whole-of-government strategy through four cyber-themed pillars representing vital national interests. The pillars draw attention to domestic strength, military security, and dependence on strategic partnerships:

1. Protect the American people, the homeland, and the American way of life
2. Promote American prosperity
3. Preserve peace through strength
4. Advance American influence<sup>88</sup>

---

<sup>84</sup> “Bureau of Diplomatic Security,” Department of State, accessed November 14, 2018, U.S. Department of State, <https://www.state.gov/m/ds/>.

<sup>85</sup> Department of State, International Cyberspace Policy Strategy, Public Law 114-113, Division N, Title IV, Sec. 402, March 2016, <https://2009-2017.state.gov/documents/organization/255732.pdf>.

<sup>86</sup> “International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms,” Department of State, accessed March 22, 2020, <https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm>.

<sup>87</sup> Valentin Weber, “Linking Cyber Strategy with Grand Strategy: The Case of the United States,” *Journal of Cyber Policy*, 3, no. 2 (August 17, 2018): 236–257, <https://doi.org/10.1080/23738871.2018.1511741>.

<sup>88</sup> White House, *The National Security Strategy of the United States of America* (Washington, DC: White House, 2017), 7, 17, 25, 27, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

The *National Security Strategy* recognizes global interconnectedness calling for innovative ways to renew the United States' competitive advantage to put "America first" by protecting its people and strengthening the nation's future position in the world. The *National Security Strategy* addresses revisionist powers (i.e., China and Russia) as key challenges to U.S. interests and values. The strategy indicates the cyber realm is shifting back to a great power struggle between nations seeking to establish their dominance over neighboring countries. The strategy outlines the innovative use of cyber to secure our borders against criminal and terrorist threats, safeguard critical infrastructure and digital networks, advance diplomacy, and achieve better technology to strengthen U.S. cyber capabilities to obtain an advantage in the global cyber stage.

In 2018, the National Security Presidential Memorandum–13 replaced PPD-20, providing new cyber authorities that are less restrictive and allowing the president of the United States to delegate (under certain circumstances) offense-based authorities across the cyber spectrum to the U.S. Secretary of Defense. Previously, offense-based operations were not authorized outside of armed conflict, requiring presidential authority, National Security Council review, and interagency coordination—a process that was not expeditious.<sup>89</sup> Although the process and plans for operations are still publicly ambiguous, unclear, and in progress, the new directive will facilitate the information network protection through offense-based measures and coordination with public, private, and international partners. The DOD will be delegated offense-based authorities within a particular mission area; however, dialogue to maintain a consensus on the "how" that will be achieved remains to be solidified.<sup>90</sup>

On April 17, 2018, Department of Homeland Security (DHS) Secretary Kirstjen Nielsen announced that the United States would be taking steps toward a more aggressive and offense-based cyber policy, with the objective of replacing previous complacency with

---

<sup>89</sup> Sydney Freedberg, Jr., "Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff," *Breaking Defense*, September 17, 2018, <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.

<sup>90</sup> Freedberg.

appropriate consequences to “call out malicious cyber behavior and to punish it.”<sup>91</sup> A day earlier, the United States and United Kingdom (UK) issued a joint statement, the first of its kind, providing warning and advice to mitigate future cyber operations and malicious attacks from state-sponsored (Kremlin-backed) Russian hackers. “Russia is our most capable hostile adversary in cyberspace so dealing with their attacks is a major priority for the National Cyber Security Centre and our U.S. allies,” said Ciaran Martin, CEO of the UK’s National Cyber Security Centre, the cyber arm of the Government Communications Headquarters.<sup>92</sup> The 2018 *National Cyber Strategy of the United States of America* not only supports a strong cyber security defense but also a shift toward deterrence, resiliency, punitive actions, collective interoperability, and collaboration with private, public, and international partners.<sup>93</sup>

Not everyone supports a U.S. offense-based cyber policy, including Brad Smith, president of Microsoft. A day after the U.S.–UK joint cyber warning, a “digital Geneva accord” was created, initially with 34 entities signing on, to declare they would not help or support any government in offense-based cyberwarfare.<sup>94</sup> The Cybersecurity Tech Accord now has over 60 companies on board, including Facebook, LinkedIn, and Amazon, to “protect and empower civilians online and to improve the security, stability and resilience of cyberspace.”<sup>95</sup> In addition, the Council on Foreign Relations (CFR), an independent

---

<sup>91</sup> Stephanie Condon, “DHS Chief: U.S. to Take More Aggressive Posture against Cyber Attackers,” April 17, 2018. <https://www.zdnet.com/article/dhs-chief-us-to-take-more-aggressive-posture-against-cyber-attackers/>. The GCHQ is located in Cheltenham, England, and works closely with UK and foreign law enforcement and intelligence agencies (MI6, MI5) to defend government systems from cyber threat, provide support to the Armed Forces, and strive to keep the public safe. “Welcome to GCHQ,” GCHQ, accessed October 28, 2018. <https://www.gchq.gov.uk/>.

<sup>92</sup> Danny Palmer, “Russian Hackers Are Attacking Home Routers, ISPs and Business Firewalls To Spy and Steal Data, Warns US, UK,” ZD Net, April 16, 2018. <https://www.zdnet.com/article/russian-hackers-are-attacking-home-routers-isps-and-business-firewalls-to-spy-and-steal-data-warns/>.

<sup>93</sup> White House, The, *National Cyber Strategy of the United States of America* (Washington, DC: White House, 2018), <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

<sup>94</sup> David Sanger, “Tech Firms Sign ‘Digital Geneva Accord’ Not to Aid Governments in Cyberwar,” *New York Times*, April 17, 2018, <https://www.nytimes.com/2018/04/17/us/politics/tech-companies-cybersecurity-accord.html>.

<sup>95</sup> “NTT Joined Cybersecurity Tech Accord, A Growing Global Industry Agreement To Protect Users And Customers Everywhere,” NTT Group, October 31, 2018. [https://www.ntt.co.jp/topics\\_e/techaccord/index.html](https://www.ntt.co.jp/topics_e/techaccord/index.html).

think tank organization, deduces that cyberattacks lack the lethality of other conventional weapons—such as air strikes, bombs, tanks, and fighter jets—and will not be able to garner the political support to prioritize funding for offense-based capabilities.<sup>96</sup> CFR’s assumption, however, is flawed: cyberspace networks are vast, transcending geographical boundaries; state actors can quickly launch cyberattacks on other countries with devastating non-lethal and lethal effects. For example, NotPetya was a Russian state-sponsored ransomware cyberattack against Ukraine to show political force.<sup>97</sup> The malware spread “automatically, rapidly, and indiscriminately,” causing over 300 Ukrainian companies worldwide \$10 billion in damages, in what one person described as, “a bombing of all our systems.”<sup>98</sup> Across the Atlantic, Maersk, a maritime company responsible for a fifth of the world’s shipping containers, was left stranded in New Jersey as a result of the destroyed data, affecting worldwide trade and commerce.<sup>99</sup> A year later, victim companies were putting millions of dollars toward technology cleanup, disrupted business, and lost sales.<sup>100</sup>

The Russian state-sponsored ransomware was meant to be destructive and it created one of the most devastating cyberattacks in internet history. NotPetya is a case study for offense-based cyber operations. The destruction path left by the ransomware could have been worse—possible lethal— affecting not only equipment that maintains livelihood, but also critical infrastructure, whereby consequences of an electrical grid power outage could have rendered hospital life-support systems inoperable. Cyberattacks like NotPetya cause global collateral damage that is invasive, disruptive, paralyzing, and nondiscriminatory.

---

<sup>96</sup> “What Do the Trump Administration’s Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?” *Council on Foreign Relations* (blog), September 10, 2018. <https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations>.

<sup>97</sup> Kim S. Nash, “One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs,” *Wall Street Journal*, June 27, 2018, <https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906>.

<sup>98</sup> Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, accessed November 3, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>; DeGuerin, “U.S. Silently Enters New Age of Cyberwarfare.”

<sup>99</sup> Alex Hern, “WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017,” *Guardian*, December 30, 2017, <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware>.

<sup>100</sup> Nash, “One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs.”

Another NotPetya could happen again on a larger scale and there may not be an appropriate defense for a similar reckless attack, which is why it may be vital to have an appropriate offense.

Distinguishing between a hostile, conventional enemy and a civilian on their computer is illogical: both can cause catastrophic damage. The methods may not be as dramatic or violent, but the results can be similar. Hypothetical example: if a Washington, DC, power grid was cyberattacked, one or more hospitals in the metropolitan area would be without electricity to run machines needed to sustain patients' lives. Contingency operations such as backup generators would be implemented, but that does not guarantee the protection of all patients who are dependent on electrical power for their support and survival; one or more citizens may die. In addition, that same targeted cyber strike on critical infrastructure may quickly escalate to retaliatory actions, both cyber as well as kinetic (conventional weapons). Cyberattacks can, indeed, have lethal consequences.

Also in 2018, the *National Cyber Strategy* released a whole-of-government approach to combat the threat of cyber actors targeting U.S. government interests and the private sector. One key component was the role of DHS in assuming the lead for federal (non-DOD and non-IC) cybersecurity and information technologies. In assuming this role, DHS will have unfettered access to all federal government systems outside of the IC and DOD and be one of the lead agencies for securing federal government systems in the cyber domain.<sup>101</sup>

On October 3, 2018, the Senate passed the Cybersecurity and Infrastructure Security Agency (CISA) Act of 2017<sup>102</sup> and on November 16, 2018, the CISA Act became public law (No. 115–278). Under this bill, DHS National Protection and Programs Directorate (NPPD) transitioned into the Cybersecurity and Infrastructure Security

---

<sup>101</sup> White House, The, National Cyber Strategy.

<sup>102</sup> The House of Representatives passed the act in December 2017. See <https://www.hsgac.senate.gov/media/majority-media/johnson-backed-legislation-to-establish-dhs-cybersecurity-agency-passes-senate>.

Agency.<sup>103</sup> The NPPD was established in 2007 and handled most of DHS cyber-related projects. In 2017, NPPD received 106,000 federal and critical infrastructure cyber-incident reports, responded to 23 on-site incidents, and identified over 129,000 cybersecurity vulnerabilities.<sup>104</sup> The CISA was transformed into a standalone agency in charge of overseeing civilian and federal cybersecurity programs. Figure 3 depicts CISA's position as a standalone agency within the DHS organizational structure.

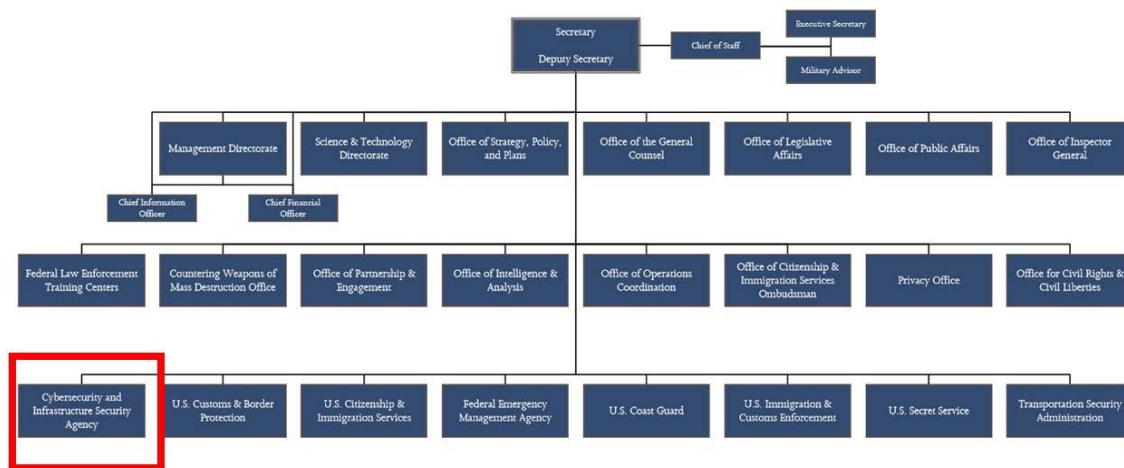


Figure 3. DHS Organizational Chart Depicting CISA (in red box)<sup>105</sup>

In an effort to deliver services to state, local, and tribal partners as well as critical infrastructure owners and operators, CISA has 10 regional offices strategically placed in close proximity, where possible, to Federal Emergency Management Agency (FEMA) offices, as shown in Figure 4.

<sup>103</sup> "Johnson-backed Legislation to Establish DHS Cybersecurity Agency Passes Senate." U.S. Senate Committee on Homeland Security and Governmental Affairs, October 3, 2018, <https://www.hsgac.senate.gov/media/majority-media/johnson-backed-legislation-to-establish-dhs-cybersecurity-agency-passes-senate>.

<sup>104</sup> "National Protection and Programs Directorate (NPPD) at a Glance," Department of Homeland Security, accessed November 15, 2018. <https://www.dhs.gov/publication/nppd-glance>.

<sup>105</sup> Adapted from "Organizational Chart," Department of Homeland Security, <https://www.dhs.gov/organizational-chart>.



Figure 4. CISA Regional Service Delivery Sections<sup>106</sup>

In addition to support modeled after FEMA’s regional structure, CISA Director Christopher Krebs is using the next two years—2019 to 2021—to mature the agency. CISA’s priorities over that timeframe include election security, government network security, potential threats from foreign virtual private networks, and keeping Chinese tech suppliers, like Huawei, out of networks using 5G mobile telecommunications.<sup>107</sup> The priorities mark an objective to harden defenses against primary adversaries, Russia and China, and mitigate risk.

The international community’s consensus to develop better cyber strategies indicates the need for the United States to step up its cyber capabilities to achieve national security objectives, collaborate with key partners, and attribute and deter cyber activities to identify hostile foreign state-sponsored cyber programs, intentions, and capabilities.<sup>108</sup> A challenge across U.S. public and private sectors is implementing current cyber policies to accomplish the president’s objectives and achieve dominant cyber presence while

<sup>106</sup> Source: “CISA Regional Service Delivery Model Fact Sheet,” Cybersecurity and Infrastructure Security Agency, accessed February 24, 2020, <https://www.cisa.gov/publication/cisa-regional-service-delivery-model-fact-sheet>.

<sup>107</sup> Cynthia Brumfield, “New CISA Director Outlines Top 5 Priorities for Protecting U.S. Critical Infrastructure,” CSO, March 6, 2019, <https://www.csoonline.com/article/3353638/new-cisa-director-outlines-top-5-priorities-for-protecting-u-s-critical-infrastructure.html>.

<sup>108</sup> White House, The, National Cyber Strategy of the United States of America.

operating within undefined rules of conduct, engagement, and confusing law of cyberwarfare.

The cyber domain present at the creation of USCYBERCOM in 2008 has significantly changed, requiring a new—or at the very least modified—approach to influence malign cyber behavior and improve U.S. national security. Until 2018, the United States operated under a more defensive policy, countering attacks as or after they entered the American sphere, as well as focusing on protection and cybersecurity.<sup>109</sup> The DOD’s cyber model used to maintain distinct, separate cyberspace and information operations (IO), but as technology and the use of the information space evolved, the DOD found it hard to maintain pace with foreign adversarial attacks that integrated their cyber activities and IO operations.<sup>110</sup>

During the USCYBERCOM’s inaugural Cyberspace Strategy Symposium at National Defense University on February 15, 2018, discussions centered around the expanded Command Vision to integrate integrating cyber and IO capabilities to influence adversarial advantages over the United States within the confines of the law. The DOD *Cyber Strategy* followed in September 2018, encompassing the “defending forward” concept to disrupt malicious cyber activity at its source through persistent offense-based engagements with adversaries that fall below the level of warfare.<sup>111</sup> The recent policy shift enables the DOD to regularly take action in cyberspace against state actors that pose strategic threats, such as Russia and China. Day-to-day cyberspace operations will be used for intelligence collection, military cyber planning, and disruption of malicious activity at its source. The strategic aim is to strengthen cyber-defense security and resiliency while actively competing against cyber competitors in an offense-based capacity to build a U.S. cyber advantage with partner agencies, industry, and international partners.

---

<sup>109</sup> David Sanger, “Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict,” *New York Times*, June 17, 2018, <https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html>.

<sup>110</sup> U.S. Cyber Command, *2018 Cyberspace Strategy Symposium Proceedings* (Fort Meade, MD: U.S. Cyber Command, 2018), <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427>.

<sup>111</sup> Department of Defense, *Cyber Strategy 2018*.

An objective in declaring an aggressive cyber domain, as is an objective across all U.S. military domains, is to “achieve and maintain superiority” against our adversaries, as well as provide notice that the United States has the capabilities to “defend and advance national interests in collaboration with domestic and foreign partners.”<sup>112</sup> The USCYBERCOM approach, as discussed in its 2018 Command Vision, is to deviate from the cyber terms “hacking” and “attacking,” labels that bin cyberattacks as mere nuisances, towards “deterrence,” acknowledging sophisticated cyber campaigns that seek to degrade U.S. power.<sup>113</sup> Cyber operations have opened a new dimension in the battlespace and can impact U.S. cyberspace dominance, presence, and power without traditional armed aggression. It is imperative that the United States lead and engage with the international community to develop and implement an effective governance structure to guide and advance national interests in the cyber domain. On May 4, 2018, President Donald Trump, under the advisement of Defense Secretary James Mattis, officially elevated the sub-command to a Unified Combatant Command in response to the growing cyberspace threat and operating environment. It is yet to be seen if USCYBERCOM’s elevation will enable it to be aggressive and forwardly defensive in the cyber fight.

The DOD built upon their cyber strategy with its *2019 Digital Modernization Strategy* as a roadmap to support the cyber strategy’s lines of effort consisting of the cloud, artificial intelligence, command, control and communications, and cybersecurity. The strategy’s objective to “increase capabilities across [the DOD] and strengthen overall adoption of enterprise systems to expand the competitive space in the digital arena” will be achieved through four main initiatives: innovation for competitive advantage, optimization, resilient cybersecurity, and cultivation of talent.<sup>114</sup> The digital modernization effort priorities and goals are depicted in Figure 5.

---

<sup>112</sup> Joint Chiefs of Staff, *Cyberspace Operations*, JP 3-12 (Washington, DC: Joint Chiefs of Staff, 2018) [https://fas.org/irp/doddir/dod/jp3\\_12.pdf](https://fas.org/irp/doddir/dod/jp3_12.pdf).

<sup>113</sup> U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort Meade, MD: U.S. Cyber Command, 2018), [https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision %20 April%202018.pdf?ver=2018-06-14-152556-010](https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010).

<sup>114</sup> Department of Defense, *DoD Digital Modernization Strategy* 2019.

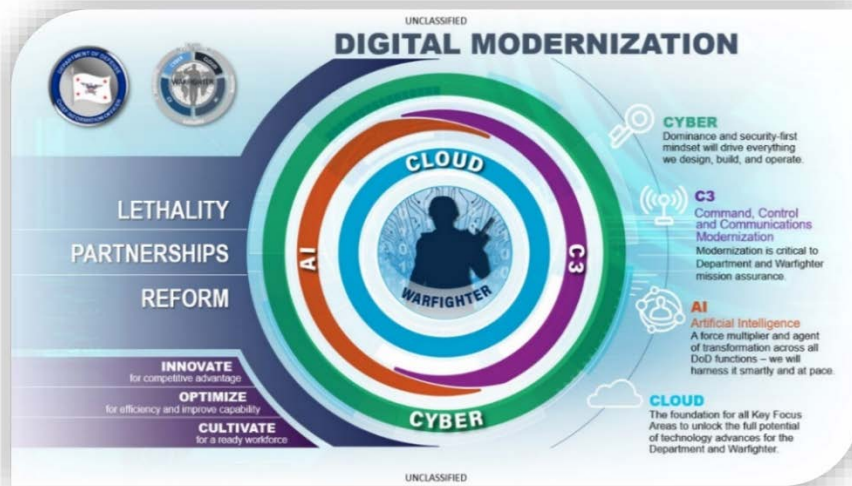


Figure 5. DOD Digital Modernization Goals (left) and Priorities (right) 2019<sup>115</sup>

It is too soon to tell if the digital modernization strategic roadmap will be successful in implementing the cyber strategy objectives. If it is successful, the DOD may see an increase in the military's cyber-technological capabilities to ensure military personnel have the tools necessary to maintain a ready workforce.

### C. THE MAIN CYBER ACTORS

There are three main subsets of actors with significant cyber capabilities that can be impacted by U.S. cyber strategy: nation-states, non-state actors, and proxies. As previously mentioned, nation-state actors—Russia, North Korea, and China—are at the forefront of cyber discussions among cyber-centric international governments, the private sector, and academia. Nation-state threats are recognized as high-end priorities critical to merit foci of national resource and response. A gap, however, pertains to information about non-state actors and proxy state actors regarding compliance and enforcement mechanisms. Both types of actors pose interesting cyber challenges because of the difficulties of attribution and accountability. For example, proxy-state actors provide a distinct governance challenge because they may be purportedly acting under the arm of a state

<sup>115</sup> Source: Department of Defense, *DoD Digital Modernization Strategy* 2019.

actor, but the state actor refuses acknowledgement of and claim to their actions. Non-state actors do not normally bear obligations under international law, a framework by which states are held responsible for actions, which makes it difficult to bind non-state actors for the wrongful acts they commit.<sup>116</sup>

## **1. Nation-State Actors**

The majority of cyber governance research and discussions cover nation-state actors. International laws, as well as the restatement of international laws into black letter rules in relation to the cyber domain as translated by the *Tallinn Manual 2.0*, pertain mostly to state actors. However, nation-state governance is interconnected with non-state and proxy state actors. Therefore, it is unwise to discuss non-state actors without briefly addressing nation-state and proxy actors. States, non-states, and proxies cannot be discussed in a vacuum. As such, this paper touches upon the nation-state issues due to the relevance to governance and interconnectedness of cyber activity but will not fully explore them to remain within scope of this paper.

Russia and China are two of the most significant adversarial nation-state actors in the cyber domain, followed by North Korea. Their priorities are to obtain governmental information to provide advantages over the United States and its allies in negotiations and decision-making. State cyberattacks include cyberespionage, cyberwarfare, election interference, misinformation campaigns, phishing, denial of service, malware, stolen information, and other types of disruptions to governments, private sectors, and civilians. In July 2019, Microsoft noted that 8,000 of its customers had been attacked by nation-states over the past year.<sup>117</sup>

One of the most significant state cyberattacks was the Stuxnet worm on an Iranian nuclear enrichment center, targeting supervisory control and data acquisition as well as

---

<sup>116</sup> Jean d'Aspremont, André Nollkaemper, Ilias Plakokefalos, and Cedric Ryngaert, "Sharing Responsibility Between Non-State Actors and States in International Law: Introduction," *Netherlands International Law Review* 62, 49–67 (2015), <https://doi.org/10.1007/s40802-015-0015-0>.

<sup>117</sup> Oscar Williams, "Microsoft Reveals Scale of Nation-State Attacks Targeting Customers," *New Statesman*, July 18, 2019, <https://tech.newstatesman.com/security/microsoft-customers-nation-state-hackers>.

uranium centrifuges. In 2012, the *New York Times* posted an article stating the worm was part of a U.S.–Israeli cyberwar program called “Operation Olympic Games” that repeated attacks for several years. The attack resulted in “the spread of a template for what computer security experts have called the most dangerous cyberweapon ever.”<sup>118</sup> Stuxnet is a significant attack because it changed the cyber landscape as it pertains to state actors with the first weaponized, targeted attack on a system thought to be isolated from cyberattacks.

## 2. Proxy State Actors

States use a variety of proxy relationships to project coercive power in cyberspace. Maurer defines cyber proxies as “intermediaries that conduct or directly contribute to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary.”<sup>119</sup> Proxy relationships typically fall under three categories: delegation, orchestration, and sanctioning (approving or permitting) with varying uses of coercive power. Table 1 displays the three proxy categories and the level of power a nation-state maintains in the proxy relationship.

Table 1. State Proxy Relationships and Level of Coercive Power<sup>120</sup>

| Proxy Category | Nation-State Power Relationship                                                     |
|----------------|-------------------------------------------------------------------------------------|
| Delegation     | Tight leash; under state’s effective control                                        |
| Orchestration  | Looser leash; strong ideational bonds; receives funding or tools                    |
| Sanctioning    | Passive support: state aware of activity of a non-state actor but turns a blind eye |

The 2014 Sony intrusion and the 2017 WannaCry ransomware cyberattack are recent examples of proxy state cyber activity. North Korea has significantly improved its offensive cyber capabilities over the past several years by taking advantage of proxy state

---

<sup>118</sup> Paul Rosenzweig, “Operation Olympic Games Legal Setback and Strategic Opportunity,” *Lawfare*, September 16, 2012, <https://www.lawfareblog.com/operation-olympic-games-legal-setback-and-strategic-opportunity-guest-post-ernesto-j-sanchez>.

<sup>119</sup> Maurer, *Cyber Mercenaries*, xi.

<sup>120</sup> Adapted from Maurer, xi-xii.

actors. The 2014 Sony studio-wide cyberattack leaked unreleased films online; posted executives' salaries and passwords; and threatened employees with intimidating messages (Figure 6).<sup>121</sup>

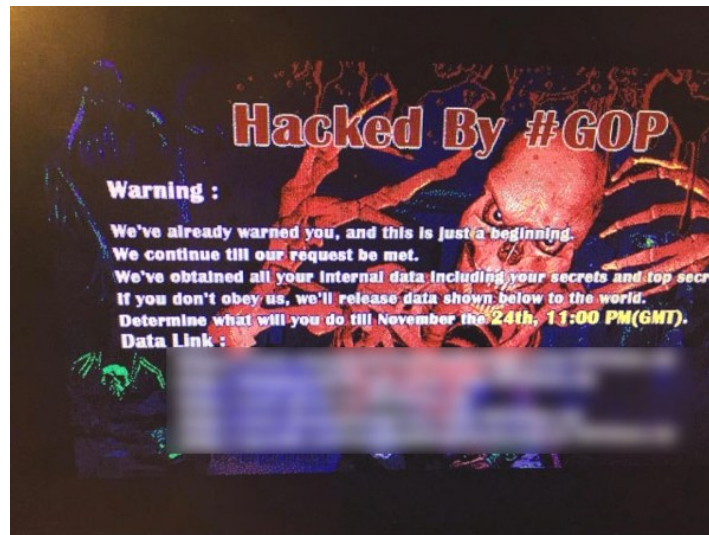


Figure 6. Example of the Intimidating Message in the 2014 Sony Attack<sup>122</sup>

The attack catapulted North Korea's evolution as a major threat in cyberspace; however, the 2017 WannaCry ransomware attack—made possible by the United States' own NSA's vulnerabilities—changed the cybersecurity game. The latter attack ramped up an evolution toward more sophisticated variations of global-scaled, multi-vectored, state-sponsored cyberattacks. Over 300,000 computers in 150 countries were infected, causing billions of dollars in damages and halting worldwide business operations.<sup>123</sup> The NSA issued an internal assessment stating Lazarus actors were sponsored by the Reconnaissance

---

<sup>121</sup> Edgar Alvarez, "Sony Pictures Hack: The Whole Story," Engadget, December 10, 2014, <https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/>.

<sup>122</sup> Timothy Seppala, "Sony Pictures Hack Takes Computers Down Studio-Wide," Engadget, November 24, 2014, <https://www.engadget.com/2014/11/24/sony-pictures-hack/>.

<sup>123</sup> "Cyber-attack: U.S. and UK blame North Korea for WannaCry," BBC, December 19, 2017, <https://www.bbc.com/news/world-us-canada-42407488>.

General Bureau, North Korea's intelligence bureau for clandestine operations.<sup>124</sup> Researchers noted that the 2017 attack “marked the shift toward using military-grade weapons, hacking tools that are powerful enough for a national cyber-defense agency to use on international cyber-warfare.”<sup>125</sup>

Russia also extensively utilizes cyber mercenaries for proxy state actions. Turla is a Russian-sponsored cyberespionage group that conducts campaigns against government institutions using internally created as well as open-source exploitation tactics in their operations.<sup>126</sup> In October 2019, the group was responsible for compromising an Iranian-backed hacking group, OilRig or APT34, by exploiting their techniques and tools and using them to attack more than 35 countries.<sup>127</sup> Initially, the attacks were attributed to the Iranian groups; however, it was later determined that Turla masked its identity through the Iranians by hijacking their IP addresses and accessing their command and control infrastructure. This case demonstrated that compromise indicators—forensic data—and identifying locations of infrastructure access can be useful in determining correct attribution.

### 3. Non-state Actors

Non-state actors are not at the forefront of cyber regulatory discussions even though they often conduct a preponderance of the malign cyber activities. Agent Ari Baranoff of the U.S. Secret Service stated “many of the [non-state] actors that we look at on a daily and weekly basis have capabilities that actually exceed the capabilities of most nation-

---

<sup>124</sup> Michael Schmitt and Sean Fahey, “WannaCry and the International Law of Cyberspace,” *Just Security*, December 22, 2017, <https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/>.

<sup>125</sup> Tara Seals, “One Year After WannaCry: A Fundamentally Changed Threat Landscape,” *Threat Post*, May 17, 2018, <https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/>.

<sup>126</sup> Doug Olenic, “Turla Cyberespionage Group Switched to Open-Source Malware,” *SC Magazine*, May 22, 2018, <https://www.scmagazine.com/home/security-news/malware/turla-cyberespionage-group-switched-to-open-source-malware/>.

<sup>127</sup> “Nation-State Actors on the DarkNet,” *DarkOwl* (blog), January 2, 2020, <https://www.darkowl.com/blog-content/nation-state-actors-on-the-darknet>; “Turla Revealed As Exploiting Iranian Hacking Tools and Techniques To Attack Dozens of Countries,” *National Cyber Security Centre*, October 21, 2019, <https://www.ncsc.gov.uk/news/turla-group-behind-cyber-attack>.

states.”<sup>128</sup> The National Intelligence Council defines non-state actors as “non-sovereign entities that exercise significant economic, political, or social power and influence at a national, and in some cases international, level.”<sup>129</sup> The *Journal of Military Studies* provides a descriptive chart of the main non-state actors within the cyber domain. Their chart in Figure 7 lists the different types of non-state actors, their motivations for attacks (e.g., political change or financial gain), preferred targets, and methods used in conducting attacks.

| Actor                     | Motivation                                | Target                                                    | Method                                                 |
|---------------------------|-------------------------------------------|-----------------------------------------------------------|--------------------------------------------------------|
| Ordinary citizens         | None (or weak)                            | Any                                                       | Indirect                                               |
| Script kiddies            | Curiosity, thrills, ego                   | Individuals, companies, governments                       | Previously written scripts and tools                   |
| Hacktivists               | Political or social change                | Decisionmakers or innocent victims                        | Protests via web page defacements or DDoS attacks      |
| Black-hat hackers         | Ego, personal animosity, economic gain    | Any                                                       | Malware, viruses, vulnerability exploits               |
| White-hat hackers         | Idealism, creativity, respect for the law | Any                                                       | Penetration testing, patching                          |
| Grey-hat hackers          | Ambiguous                                 | Any                                                       | Varying                                                |
| Patriot hackers           | Patriotism                                | Adversaries of own nation-state                           | DDoS attacks, defacements                              |
| Cyber insiders            | Financial gain, revenge, grievance        | Employer                                                  | Social engineering, backdoors, manipulation            |
| Cyber terrorists          | Political or social change                | Innocent victims                                          | Computer-based violence or destruction                 |
| Malware authors           | Economic gain, ego, personal animosity    | Any                                                       | Vulnerability exploits                                 |
| Cyber scammers            | Financial gain                            | Individuals, small companies                              | Social engineering                                     |
| Organized cyber criminals | Financial gain                            | Individuals, companies                                    | Malware for fraud, identity theft, DDoS for blackmail  |
| Corporations              | Financial gain                            | ICT-based systems and infrastructures (private or public) | Range of techniques for attack or influence operations |
| Cyber espionage agents    | Financial and political gain              | Individuals, companies, governments                       | Range of techniques to obtain information              |
| Cyber militias            | Patriotism, professional development      | Adversaries of own nation-state                           | Based on the group capabilities                        |

Figure 7. Main Non-state Actors in Cyberspace.<sup>130</sup>

<sup>128</sup> Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press: 2018), x.

<sup>129</sup> National Intelligence Council, “Nonstate Actors,” 2.

<sup>130</sup> Source: Johan Sigholm, “Non-State Actors in Cyberspace Operations,” *Journal of Military Studies*, Vol. 4 Issue 1, 11, November 23, 2016, <https://doi.org/10.1515/jms-2016-0184>.

Terrorists, terrorist supporters and sympathizers are also considered non-state actors. The FBI defines international terrorism as “violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations” and domestic terrorism as similar acts to “further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.”<sup>131</sup> For the purposes of this thesis, non-state actor categorization will align with the National Intelligence Council, *Journal of Military Science*, and FBI to include hackers, hacktivists, terrorists, and cybercriminals, and their related organizations, who act according to their own agenda and ideologies without any ties to or support from nation-states.

The United States serves as an integral component of non-state cyber governance. The FBI’s Cyber Division is the lead U.S. federal agency for investigating cyberattacks and intrusions onto government and private networks by non-state actors such as criminal organizations, terrorists, and other cyber adversaries. In January 2015, alleged Pro-Islamic State of Iraq and Syria (ISIS) hackers compromised USCENTCOM’s Twitter and YouTube accounts. The terrorist sympathizers dubbed the “CyberCaliphate” accessed CENTCOM’s unclassified, commercial non-DOD servers for approximately 30 minutes, posting a picture of an ISIS fighter with the words, “i love you isis” and “AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK” (Figure 8).<sup>132</sup>

---

<sup>131</sup> Federal Bureau of Investigations, “What We Investigate: Terrorism: Terrorism Definitions.” accessed January 13, 2020. <https://www.fbi.gov/investigate/terrorism>.

<sup>132</sup> Paul McLeary, “Pentagon: Hacking of CENTCOM Site a Prank,” Defense News, January 12, 2015, <https://www.defensenews.com/opinion/intercepts/2015/01/12/pentagon-hacking-of-centcom-site-a-prank/>.



Figure 8. Compromised U.S. CENTCOM Twitter Page<sup>133</sup>

The Pentagon confirmed the attack, calling it a “prank” and labeled it cyber vandalism.<sup>134</sup> Although USCENTCOM stated no classified information was posted, phone numbers and email addresses of personnel were listed during the 30-minute duration before taken down. Doubts have been raised pertaining to attribution; regardless of whether the attack was conducted by the CyberCaliphate or another non-state actor(s), it demonstrates the feasibility and low-cost measures that can make a mark on cyber infrastructure.

Another example of the United States’ involvement in non-state cyber regulatory measures was the 2016 Avalanche case. The U.S. Department of Justice announced in December 2016 that its Cyber Division, along with the FBI Criminal Division, Western District of Pennsylvania U.S. Attorney’s Office, Germany’s Public Prosecutor’s Office and local police, Europol, investigators and prosecutors from more than 40 global jurisdictions, and numerous other entities partnered to dismantle a criminal infrastructure—Avalanche—through a multinational operation that resulted in arrests in four countries.<sup>135</sup> Avalanche

<sup>133</sup> Adapted from Josh Constine, “ISIS CyberCaliphate Hacks U.S. Military Command Accounts,” TechCrunch, January 12, 2015, <https://techcrunch.com/2015/01/12/cyber-caliphate/>; Helene Cooper, “ISIS Is Cited in Hacking of Central Command’s Twitter and YouTube Accounts,” *New York Times*, January 12, 2015, <https://www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html>.

<sup>134</sup> McLeary, “Pentagon: Hacking of CENTCOM Site a Prank.”

<sup>135</sup> Assistance was provided by DHS U.S.-Computer Emergency Readiness Team (US-CERT), the Shadowserver Foundation, Fraunhofer Institute for Communication, Registry of Last Resort, ICANN and global domain registries, DOJ Criminal Division’s Office of International Affairs, as well as India, Singapore, Taiwan and Ukraine. Department of Justice, Office of Public Affairs, “Avalanche Network Dismantled in International Cyber Operation,” Press Release No.: 16-1422, December 5, 2016.

was a cybercriminal network, accessed through criminal underground online forums, that provided a secure infrastructure for criminal campaigns and transactions, such as malware money laundering “money mule” schemes outside of the purview of law enforcement. Since 2010 when Avalanche became operational, the network redirected stolen financial information from up to 500,000 malware-infected computers daily, causing worldwide monetary losses estimated to be in the hundreds of millions of dollars.<sup>136</sup> This case is an example of the United States collaborating with international law enforcement partners to take down organized cybercrime. In this case, jurisdiction was determined based on the location of malware attack victims in the Western District of Pennsylvania. To bring the case forward for prosecution, the Department of Justice relied on a temporary restraining order for violations of Title 18 U.S.C. §§ 1343, 1344, and 2511, without which the unlawful actions would continue, causing “irreparable harm to both individuals and businesses in the United States.”<sup>137</sup> GozNym was one of the malwares used by the Avalanche criminals. On September 8, 2016, Krasimir Nikolov was arrested in Bulgaria and extradited to the United States for his connection with the GozNym malware. On October 4, 2016, Nikolov was indicted in the U.S. District Court for the Western District of Pennsylvania as a conspirator of unauthorized access of a computer to obtain financial information, bank fraud, and criminal conspiracy.<sup>138</sup> The Avalanche network supported more than 800,000 domains that facilitated criminal money mule transactions between the malware victims and the cybercriminals.

The Avalanche case demonstrates the need for a multi-lateral, multipronged regulatory mechanism for non-state cyber activities. The United States faces a multitude

---

<sup>136</sup> Department of Justice, Office of Public Affairs.

<sup>137</sup> *Plaintiff v. “flux” a./k/a “ffllost,” and “fltJx2” alWa”ffhost2,” Defendants*, Temporary Restraining Order to Show Cause (United States District Court, Western District of Pennsylvania, November 2016), <https://www.justice.gov/opa/page/file/915226/download>; Section 1343 pertains to wire fraud and the use of electronic communication made in furtherance of the scheme, Section 1343 pertains to bank fraud—defrauding a federally chartered or insured financial institution or to obtain any of the monies, funds, credits, assets, securities, or other property owned by, or under the control of, such an institution, Section 2511 prohibits the unauthorized interception, disclosure, and use of wire, oral, or electronic communications, “Criminal Resource Manual,” Department of Justice, accessed February 22, 2020, <https://www.justice.gov/archives/jm/criminal-resource-manual>.

<sup>138</sup> *United States v. Krasimir Nikolov*, Indictment, (United States District Court, Western District of Pennsylvania, 2016) <https://assets.documentcloud.org/documents/3251405/Nikolovindict-1.pdf>.

of significant threats from multiple capable state, proxy state, and non-state actors that rank above a single nation-state. There needs to be greater cooperation and coordination among U.S. and international governments, private sectors, and academic partners to properly address these complex threats.

### III. RULES OF ENGAGEMENT, INTERNATIONAL LAW, AND CYBERSPACE

In order to determine an effective regulatory mechanism for cyberspace, it is necessary to understand cyber concepts as they currently exist. This chapter begins with an overview of the law of war (LOW), a concept integral to governance. Although the regulatory mechanisms explored and proposed in this thesis pertain to peacetime activities, it is essential to understand LOW at a high level as an integral part of the holistic cyber governance picture. Next, the chapter examines the principle sections of international law as restated in the *Tallinn Manual 2.0*, followed by the Budapest Convention, the first international treaty on cybercrime. Both are frameworks to consider and evaluate in Chapter IV when developing a cyber regulatory mechanism. The chapter concludes with a look at the functions of the UN and NATO, two organizations involved in global crisis management, peace, and security cooperation. The organizational subsections provide a foundation of knowledge leading in to Chapter IV's determination of a single or multiple-entity regulatory mechanism.

The international community needs to develop common understandings about how the rules and law of armed conflict apply—or do not apply—and what should be done in this area. The cyber domain is not a lawless space free from rules and compliance.<sup>139</sup> Nations widely agree that established principles of international law do apply in cyberspace; the question remains *how* should they apply, what changes or additions need to be made based on the landscape, and how should they be governed?<sup>140</sup> An international governing body or mechanism serves as the umbrella entity that fosters the collaborative partnerships and relationships prior to cyber crises and adverse cyber events. Once established, the trickle-down effect will provide significant guidance in developing U.S. policies and procedures for domestic regulation and international compliance within the cyber domain.

---

<sup>139</sup> Koh, “International Law in Cyberspace.”

<sup>140</sup> Koh.

The first step in examining application of international law to cyber actors is to evaluate the existing application of international law to state actors in the traditional sense; then, the next step is to determine whether such laws similarly apply to non-state actors in the cyber domain.

## **A. LAW OF WAR OVERVIEW**

For the purpose of this paper, an overview of ROE and LOW are provided along with their application to the cyber domain. ROE are necessary across each of the five battlespace domains to mitigate conflict and ensuing consequences of escalating attacks.<sup>141</sup> In the rapidly changing cyber domain, state actors such as Russia and North Korea are pushing the boundaries of warfare, which leads to the questions: What are the boundaries of cyber warfare? Should cyber warfare ROE align with international and U.S. military ROE or should cyber ROE be unique to the digital cyber domain?

Fear looms that a proactive, offense-based U.S. cyber environment may prompt retaliatory cyber operations, leading to increased costs due to cyclical, reactive cyber operations and increased vulnerabilities. The United States holds an advantage in conventional military domains that may sway and “may prompt U.S. adversaries to seek other (non-cyber) asymmetric—and potentially effective—means of contesting or responding to U.S. behavior in cyberspace.”<sup>142</sup> Physical, conventional operations can be measured and observed by the augmentation of troops, weaponry, and aircraft over days and weeks. Kinetic operations require training and expertise to handle the weapons as well as funding to support the activity. Asymmetric cyber operations differ because the development of attack is hard to observe; the cyber weapon is hard to trace and detect, making attribution difficult; execution of attacks does not require a high degree of expertise; and funding is not necessary for successful execution. The ability to cause major damage with minor resources makes cyber operations favorable over traditional warfare. The accessibility and feasibility for non-state actors to carry out asymmetric cyber

---

<sup>141</sup> The five battlespace domains are land, air, sea, cyber, and space.

<sup>142</sup> Council on Foreign Relations, “What Do the Trump Administration’s Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?”

operations places the United States and international community in a position to have their vulnerabilities exploited.

Offense-based strategies carry the risk of conflict with foreign states in cyberspace and could lead to retaliatory adversarial responses, spiraling into a back-and-forth cyber battle due to the lack of clear rules of conduct, mechanisms, and methods for escalation control. Military doctrine expanded its battle domains beyond air, land, and sea to include space and cyberspace.<sup>143</sup> As a result of unclear thresholds, a line of thought among the international community is that cyber conflicts could quickly escalate, becoming kinetic, “because of misperception or miscalculation.”<sup>144</sup> Recent hacking attacks such as Sony and the U.S. presidential election highlight the complexities involved when official ROE do not exist; questions arise as to when the line defining cyberwarfare is crossed and when, as well as how, a consistent, effective, and expedient response should be issued.<sup>145</sup> Although there have been extensive international, intergovernmental, and public discussions about ROE and LOW as it applies to cyber warfare, no publicly available, well-defined ROE or protocols for offense-based, aggressive responses to cyberattacks currently exist to guide nations’ behavior.

According to the Joint Chiefs of Staff Publication (JP) 1–04, LOW is defined as that part of war that “regulates the conduct of states and combatants engaged in armed hostilities” with the purpose to “prevent unnecessary suffering, safeguard certain fundamental human rights of those involved in a conflict, and to ultimately restore peace.”<sup>146</sup> The LOW, also known as the *law of armed conflict*, encompasses all international law for conflict of which the United States is a part, including treaties and

---

<sup>143</sup> Joint Chiefs of Staff, *Cross-Domain Synergy in Joint Operations*, 1.

<sup>144</sup> Adam Segal, “An Update on U.S.-China Cybersecurity Relations,” *Council on Foreign Relations* (blog), November 17, 2017. <https://www.cfr.org/blog/update-us-china-cybersecurity-relations>.

<sup>145</sup> “The Time Has Come for Rules of Engagement for Cyberwarfare,” Infosec Institute, II-2, accessed November 15, 2018. <https://resources.infosecinstitute.com/the-time-has-come-for-rules-of-engagement-for-cyberwarfare/#gref>.

<sup>146</sup> Joint Chiefs of Staff, *Legal Support to Military Operations*, JP 1-04 (Washington, DC: Joint Chiefs of Staff, 2016), [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_04.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_04.pdf); U.S. Marine Corps Basic School, *Law of War/Introduction to Rules of Engagement B130936 Student Handout* (Camp Barrett, VA: United States Marine Corps), <https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B130936%20Law%20of%20War%20and%20Rules%20Of%20Engagement.pdf>.

agreements, and is binding on the United States and its citizens.<sup>147</sup> As stated in JP 1-04, its purpose is to facilitate peace, provide humanitarian safeguards for all classes of civilians, combatants, and noncombatants as well as to prevent the escalation of conflict into cruel violence if peace cannot be immediately achieved. Under Title 10, USC Section 156, the assigned legal counsel to the Chairman of the Joint Chiefs of Staff is responsible for reviewing and advising on LOW and ROE as they relate to cyberspace operations.<sup>148</sup> In 2017, Secretary of Defense James Mattis loosened the requirements for ROE to enable the U.S. military to move more quickly against terrorist organizations.<sup>149</sup> Previously, troops had to be in contact with the enemy, or were bound by proximity, before they could strike; this requirement has been removed.<sup>150</sup> Terrorists and state actors are hostile adversaries with lethal capabilities wishing to cause harm to the United States. If the United States follows military ROE for the cyber domain, this update could support current U.S. policies calling for more aggressive cyber operations.

Figure 9 provides a chart to understand the comparison between traditional and cyber warfare domains. Based on this chart, an assumption can be made that cyber warfare will become favorable to U.S. adversaries due to inexpensive resources, challenging attribution, cross-sector environment, and collateral effects that are global in nature.

---

<sup>147</sup> Joint Chiefs of Staff, *Implementation of the DoD Law of War Program*, CJCSI 5810.01D (Washington, DC: Joint Chiefs of Staff, 2010), <http://www.jcs.mil/LinkClick.aspx?fileticket=xsR7uIFHy4o%3D&tabid=19767&portalid=36&mid=46626>.

<sup>148</sup> Legal Counsel to the Chairman of the Joint Chiefs of Staff, 10 *U.S. Code* § 156 (2008) <https://www.law.cornell.edu/uscode/text/10/156>.

<sup>149</sup> Aaron Mehta, "Mattis Reveals New Rules of Engagement," *Military Times*, October 3, 2017, <https://www.militarytimes.com/flashpoints/2017/10/03/mattis-reveals-new-rules-of-engagement/>.

<sup>150</sup> Mehta.

| Characteristic                   | Cyberspace Domain                                                                                                                                                                                                         | Traditional Domains                                                                                                                                                                                      |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resources                        | <ul style="list-style-type: none"> <li>• Inexpensive relative US air, land and sea</li> <li>• Human capital-driven</li> </ul>                                                                                             | <ul style="list-style-type: none"> <li>• Limited to nations with significant financial resources</li> <li>• Industrial-based assets</li> </ul>                                                           |
| Physical                         | <ul style="list-style-type: none"> <li>• Artificial construct, permeable virtual boundaries</li> <li>• Multi-use environment (government, military, commercial)</li> <li>• Distributed, dynamic and non-linear</li> </ul> | <ul style="list-style-type: none"> <li>• Exists naturally, discrete physical boundaries</li> <li>• Multi-use environment (government, military, commercial)</li> </ul>                                   |
| Actors                           | <ul style="list-style-type: none"> <li>• Ambiguous</li> <li>• From nation-states to individuals to criminal organizations to commercial entities</li> </ul>                                                               | <ul style="list-style-type: none"> <li>• Identity of adversary usually known</li> </ul>                                                                                                                  |
| Effects                          | <ul style="list-style-type: none"> <li>• Global in nature</li> <li>• Non-Kinetic or Kinetic</li> <li>• Collateral damage on 2nd/3rd order effects potentially global</li> </ul>                                           | <ul style="list-style-type: none"> <li>• Usually regionally focused (Space is exception)</li> <li>• Usually Kinetic (EW exception)</li> <li>• Collateral damage limited to active battlespace</li> </ul> |
| Authorities for Offensive Action | <ul style="list-style-type: none"> <li>• Elevated</li> <li>• Evolving ROE</li> </ul>                                                                                                                                      | <ul style="list-style-type: none"> <li>• Local</li> <li>• Establish ROE</li> </ul>                                                                                                                       |
| Intelligence Support             | <ul style="list-style-type: none"> <li>• Requires knowledge of adversary capabilities and intent</li> <li>• Compressed timeline (“net” speed)</li> <li>• Attribution is challenging</li> </ul>                            | <ul style="list-style-type: none"> <li>• Requires knowledge of adversary capabilities and intent</li> </ul>                                                                                              |

Figure 9. List of Characteristics Comparing Cyber Domain vs. Traditional Warfare Domains<sup>151</sup>

When a devastating cyberattack occurs, for example, disabling large-scale power grids across the country, when and how do the ROE and LOW apply? Does the current policy allow for a kinetic troops-on-the-ground war? Do we respond in kind? Or, is it a case-by-case basis decided by our national policymakers? The answers to these questions may only be known in fragments or behind classified closed doors.

The chart in Figure 10 depicts information (cyber) and kinetic (traditional) warfare along a spectrum, with all actions falling between purely kinetic or purely informational. Any actions above the red line (threshold for declaring war) are the most severe; for example, a cyberattack that destroys the national power grid (highest severity for

<sup>151</sup> Source: Sean Brandes, “The Newest Warfighting Domain: Cyberspace,” *Synesis Journal of Science, Technology, Ethics, and Policy*, G-94 (2013), [http://www.synesisjournal.com/vol4\\_g/Brandes\\_2013\\_G90-95.pdf](http://www.synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf).

information warfare) or a nuclear strike (highest severity for kinetic warfare).<sup>152</sup> More cyber than kinetic actions fall in the gray section denoting legal ambiguity with respect to international law.

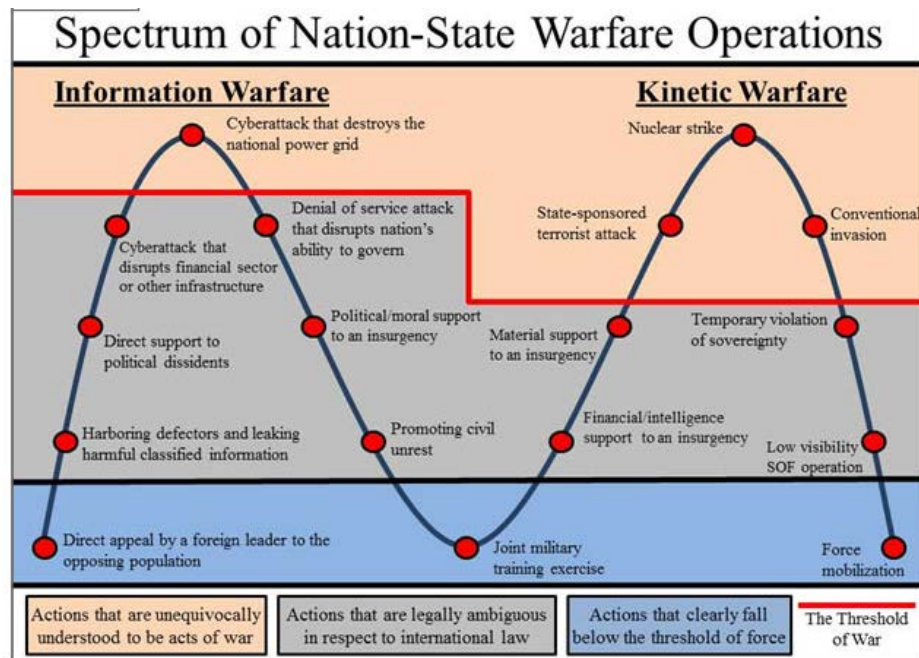


Figure 10. Information and Kinetic Warfare Spectrum Chart<sup>153</sup>

At present, gaps still remain regarding cyberwarfare ROE and LOW. UN Secretary-General Antonio Guterres has stated in two separate speeches to the delegation that “there is no regulatory scheme for [cyber] warfare” because “it is not clear how the Geneva Convention [s] or international humanitarian law applies.”<sup>154</sup> Articles 2 and 3 of the Geneva Convention of 1949—international rules that apply during armed conflict—provide that war may be declared when there is partial or total occupation of territory,

<sup>152</sup> Jason Rivera, “Understanding and Countering Nation-State Use of Protracted Unconventional Warfare,” *Small Wars Journal*, accessed February 22, 2020, <https://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare>.

<sup>153</sup> Source: Rivera.

<sup>154</sup> David Fidler, “The UN Secretary-General’s Call for Regulating Cyberwar Raises More Questions Than Answers,” Council on Foreign Relations, March 15, 2018, <https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers>.

armed conflict between two or more parties, or conflict between states whereby war is not recognized between them. The UN broadly interprets “war” as any nonconformity with the “principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.”<sup>155</sup> By this definition, is knocking out a power grid a “nonconformity”?

In USCYBERCOM’s Command Vision, two primary risks are discussed: 1) laser-like focus on highly capable state actors will shift resources and attention from other cyber actors; 2) the United States is viewed as aggressive in the international community and an offense-based assertion may be perceived as militarization of the cyber environment. USCYBERCOM briefly explains mitigation of these risks through system resiliency, intelligence sharing, and augmented relationships with law enforcement, IC, the homeland security enterprise, and coalition partners and, increased outreach with the public to communicate adversarial threats, actions, and the U.S. emphasis on civil liberties.<sup>156</sup> The declaration of cyberspace as an operational domain does not guarantee that those associations will immediately and fully garner support for such operations due to fear of inadvertent consequences such as escalation, unnecessarily militarizing cyberspace, and jeopardizing the relationships upon which the United States is dependent.<sup>157</sup> Offense-based operations will require persistent collaboration with government, military, and private-sector entities to shape perceptions in favor of USCYBERCOM’s objectives and develop widespread support.

The Cybersecurity Tech Accord arose to protect against offense efforts and is a promise by members to forgo cyber warfare. Tampering or exploiting a Microsoft or Google vulnerability, for example, would be in violation of this agreement. The objective of the Cybersecurity Tech Accord is to provide a highlight of current and future threats to customers; prioritize security, privacy, and reduce vulnerabilities; enhance global response to threats; and protect “against exploitation of technology products and services during

---

<sup>155</sup> “United Nations and the Rule of Law,” United Nations, accessed October 4, 2018, <https://www.un.org/ruleoflaw/what-is-the-rule-of-law/>.

<sup>156</sup> U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 10.

<sup>157</sup> Brandes, “The Newest Warfighting Domain: Cyberspace,” G:94.

their development, design, distribution and use.”<sup>158</sup> Although the Cybersecurity Tech Accord arose out of a desire to set cyberspace norms of behavior and cyberwarfare rules of conduct, the accord is missing signers from key countries responsible for devastating state-sponsored cyberattacks, including Russia, China, North Korea, and Iran.<sup>159</sup> The agreement is a challenge to U.S. efforts in garnering worldwide support across the private sector.

The United States has national and global strategic interests in understanding and mitigating these offense-based cyber policy risks. The world depends on networked systems for homeland security missions, critical infrastructure, health care systems, commerce, and modern-day living. The longer it takes to implement cyber norms, including ROE, the greater the likelihood of unnecessary military escalation and diplomatic severance in and outside of the cyber domain.

State, true non-state, and proxy actors can use cyberattacks in the context of military-styled operations above the threshold for cyber warfare. LOW consists of *jus ad bellum* and *jus in bello*.<sup>160</sup> Similar to the consensus that international law in general should apply to the cyber domain, there is consensus that the tenets of *jus in bello* and *jus ad bellum* should apply to cyber warfare. *Jus in bello* and *jus ad bellum* generally operate independently of each other. *Jus ad bellum* is essential to determining whether to resort to war based on an aggressive measure, with determining principles including a “competent authority to order the war for a public purpose; a just cause (such as self-defense); the means must be proportionate to the just cause; all peaceful alternatives must have been exhausted; and a right intention on the part of the just belligerent.”<sup>161</sup> *Jus in bello* as defined by the DOD in its 2016 *War of Law Manual* is “law [applied to both defenders and aggressors] relating to the conduct of hostilities and the protection of war victims ... [and

---

<sup>158</sup> “Objective,” Cyber Tech Accord, accessed October 31, 2018. <https://cybertechaccord.org/about/>.

<sup>159</sup> Sanger, “Tech Firms Sign ‘Digital Geneva Accord’ Not to Aid Governments in Cyberwar.”

<sup>160</sup> William V. O’Brien, *The Conduct of Just and Limited War* (Westport, CT: Praeger Publishing, 1981), 9.

<sup>161</sup> Department of Defense, *Law of War Manual* (Washington, DC: Department of Defense, 2016), 82, <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>.

is] applicable to the United States, including treaties to which the United States is a Party, and applicable customary international law.”<sup>162</sup> An aggressor or defender can be in compliance with *jus in bello* but not be legally justified for military operations under *jus ad bellum*. According to *Law of War Manual*, “when no specific rule applies, the principles of LOW form the general guide for conduct during war.”<sup>163</sup> The tenets of *jus in bello* and *jus ad bellum*, along with the Geneva Conventions (1949 and amended) and Rules of Engagement (ROE) are rooted in the Just War Tradition—agreed-upon morals, ethical codes, and customary norms for justifications and limitations warfighting.<sup>164</sup>

A weapon is a weapon, whether it is a hacker using a computer or a bomb dropped from an airplane. Traditional LOW applies to cyberspace but the topic is unsettled and heavily debated to determine what counts as use of force within the meaning of *jus ad bellum* and in conducting a cyberwar (*jus in bello*). Offense and defensive principles can become blurred in cyber, especially with secrecy and attribution posing a noticeable challenge and risk not prevalent traditional conventional warfare.

## **B. RESTATEMENT OF LAW: TALLINN MANUAL 2.0’S EXAMINATION**

The *Tallinn Manual 2.0* provides comprehensive information on how international laws apply to the cyber domain during peace time. Although the manual is nonbinding and merely a restatement of the application and interpretation of international laws, it provides understanding and commentary for approaching the translation of the black letter rules—accepted basic principles of law that are no longer subject to dispute—to states, and thereby non-state actors within the cyber domain. The manual provides a framework that explores applicable general principles of international law, the law of state responsibility, the law of the sea, international telecommunications law, space law, diplomatic and consular law, and, with respect to individuals, human rights law.

---

<sup>162</sup> Department of Defense, 1.

<sup>163</sup> Department of Defense.

<sup>164</sup> Department of Defense.

However, neither *Tallinn Manual* restates the laws according to states' interpretation; they restate the law as it was interpreted by experts in their own views. The intent "was never to make law or to produce a manual that would have the force of law" but rather reflect the law at the time (*lex lata*).<sup>165</sup> Regardless, *Tallinn 2.0* is a valuable reference book and starting point for cyber regulatory conversations. The scope of *Tallinn 2.0* touches upon *jus ad bellum* and *jus in bello* as a follow-on to the original *Tallinn Manual*, but the bulk of the manual provides rules and commentary on international law for cyber operations *during peacetime*.

During the process to finalize *Tallinn 2.0*, more than 50 states—including all permanent members of the UN Security Council—participated in meetings where they had the opportunity to review and comment on the manual's content.<sup>166</sup> While the states' insights are not included in the manual, since it is written from the views of the IGE, understanding how each commenting state viewed the implementation of international law regarding cyber activity was valuable nonetheless.<sup>167</sup> In addition, the IGE sought commentary from peer reviews, thus providing a unique, robust source based on comprehensive views and expertise. The manual lists all IGE and other participants affiliated with the project, including individuals who contributed draft text for consideration. The project consisted of editors: legal experts from a wide variety of places such as Amsterdam, Tel Aviv, Wuhan (China), the International Law Commission of the UN, Tasmania, Tokyo, and the U.S. Department of State; a technical expert from NATO CCDCOE, a non-voting observer from NATO; contributors from various U.S. and international universities and military institutions; and 58 legal peer reviewers.

*Tallinn 2.0* is broken into four main parts: general international law and cyberspace, specialized regimes of international law and cyberspace, international peace and cyber

---

<sup>165</sup> *Lex lata* means "the law as it exists" or the current law compared to *lex feranda* which means "the law as it should exist" or future law. Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law*, 738, no. 48, <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf>.

<sup>166</sup> Permanent members of the UN Security include China, France, Russian Federation, the United Kingdom, and the United States.

<sup>167</sup> Jensen, "The Tallinn Manual 2.0: Highlights and Insights," 740.

activities, and the law of cyber armed conflict. Each part is divided into several sections with their associated rules. As mentioned previously, LOW/cyber armed conflict as a complex space on its own lies beyond the scope of this thesis. In this regard, understanding how the IGE restated the definitions of use of force and threat of force to understand the proposed limits of that threshold in defining the non-conflict space is important. Part I is examined as it relates to the cyber landscape, understanding nation-states, and its application to non-state actors. The remaining parts are discussed as they directly relate to this thesis in the interest of maintaining a narrow scope. For instance, “Part II: Specialized Regimes of International Law and Cyberspace,” is instrumental to understanding the restatements of international law as they apply to international human rights law, diplomatic and consular law, law of the sea, air law, space law, and international communications law. However, a thorough examination of these topics is more conducive to an analysis of specialized topic areas for process and procedure development once an international governing mechanism is determined and is not within the scope of this thesis.

“Part I: General International Law and Cyberspace” is essential to the foundation of international law, learning the main components of international law, and understanding how those components can translate into another domain. Part I consists of sovereignty, due diligence, jurisdiction, law of international responsibility, and cyber operations not regulated by international law per se.

### **1. State Sovereignty in Cyberspace**

In Part I, the IGE examined general principles of sovereignty, violations, sovereign immunity, and inviolability. The principle of sovereignty is a key foundational component of international law and one that must be critically examined and understood in its application to cyberspace. In particular, “states enjoy sovereignty over *any cyber infrastructure located on their territory and activities associated with that cyber infrastructure* [emphasis added].”<sup>168</sup> Integral to the sovereignty principle is the concept of territoriality—the use of physical territory bounds in state strategies to establish

---

<sup>168</sup> Michael Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: Cambridge University Press, 2017), 11.

jurisdiction. Cyberspace has been considered the fifth domain, joining air, land, sea, and space for military operations, but its lack of physical, tangible borders in a virtual realm enable it to be analyzed and treated similarly to the law of the seas or outer space. However, the *Tallinn 2.0* IGE disregarded the borderless arguments and noted that cyber has territorial aspects by occurring on physical objects, on existing territories, or as conducted by persons or organizations over which nation-states may exercise sovereignty.<sup>169</sup> In essence, although cyber activity can cross multiple borders, persons within or as part of infrastructure subject to the jurisdiction of one or more states conduct it, and therefore the principle of sovereignty covers the physical, logical, and social layers of cyberspaces. No one state can claim sovereignty over the whole of cyberspace since the majority of a state's cyber infrastructure lies within the bounded territory of the state.

*Tallinn 2.0* Rules 2 and 3 pertain to internal and external sovereignty, which are inextricable elements of sovereignty. A state has internal sovereignty over the cyber infrastructure, persons, and activities within its territory, unless contradicted by binding international law, such as human rights.<sup>170</sup> This sovereignty carries legal consequences: foremost, a state has domestic and legal regulatory control over all cyber infrastructure, activities, and persons within its territory (as previously defined); and second, such sovereignty and control affords the state the legal right under international law to protect its cyber infrastructure and activity within its territory, irrespective of state or private sector nature, natural and legal persons, or even the nationality of the actor.<sup>171</sup> A state may restrict certain content and impose limitations via domestic laws; however, state censorship of cyber activities fall under international human rights law and must not be discriminatory or unauthorized, or if it is, be within customary or treaty law. For example, states may not exercise their sovereignty over another state's non-commercial government authorities (i.e., heads of state, foreign ministers, or diplomatic personnel).<sup>172</sup>

---

<sup>169</sup> Schmitt, 12.

<sup>170</sup> Schmitt, 13.

<sup>171</sup> An example *Tallinn 2.0* uses is: A state enjoys sovereignty over a private ISP's server located on its territory even if the ISP is domiciled abroad. Schmitt, 13, 14.

<sup>172</sup> Schmitt, 15.

The IGE leverages the UN Charter principle of equal rights and self-determination of peoples. According to Chapter 1, Article 2(1) of the charter, the principle of sovereignty applies equally to nation-states, meaning no state has political, personal, or territorial supremacy over another state.<sup>173</sup> However, the IGE also agreed that sovereignty does not apply to international *organizations*. States are independent and as such, free to engage in cyber activities within and beyond their territory so long as they stay in the confines of international law. This activity includes entering into or abstaining from cyber agreements and treaties. In particular, Rule 3 (2) notes that a state is “not obliged to agree to particular treaty rules governing the cyber activities of its organs or nationals or conduct taking place *in its sovereign territory*” as long as another state’s sovereignty is not violated through intervention, use of force, or by any other manner.<sup>174</sup>

Rules 4 and 5 address violations of one state’s sovereignty by another state. The rules aver that any cyber interference by a state with sovereign immunity constitutes a violation of sovereignty. Intent is not an element of breach; a state may not intend its activities to result in consequences that breach a state’s sovereignty, but nevertheless, sovereignty is violated. Rule 4 avers that cyber operations must not “prevent or disregard another State’s exercise of its sovereign prerogatives” as they violate state sovereignty and, in turn, international law.<sup>175</sup> Be aware, however, the IGE agreed the rule only applies to states and *does not* apply to non-state actors *unless the non-state activities are attributable to the State* (i.e., proxy actors).<sup>176</sup> Only states must adhere to the principle of sovereignty and, therefore, only states can breach the principle of sovereignty; truly non-state actors are exempt from this rule. This exemption does not condone their actions or deem them lawful; it also does not prevent the violated state from responding to harmful non-state cyber activities pursuant to international laws based on plea of necessity, self-defense, or

---

<sup>173</sup> “Chapter I: Purposes and Principles,” United Nations, Article 2(1), <https://www.un.org/en/sections/un-charter/chapter-i/index.html>.

<sup>174</sup> Schmitt, *Tallinn 2.0*, 17.

<sup>175</sup> Schmitt, 17.

<sup>176</sup> Schmitt, 17.

countermeasures as a result of a state's failure to comply with due diligence in enabling a non-state actor to operate within its territory.<sup>177</sup>

Certain objects may enjoy sovereign immunity and, in turn, inviolability. Leveraging the Law of the Sea Convention, the IGE stated that international law accords sovereign immunity to any object, cyber infrastructure, platform, or person devoted exclusively to non-commercial, government cyber purposes.<sup>178</sup> Despite sovereign immunity, the principle of sovereignty in international law applies, particularly the obligation to respect the sovereignty of another state. If there is interference or disruption of the object, infrastructure, or platform, sovereign immunity is violated.

## **2. Due Diligence**

The general international law principle of due diligence must also apply to cyberspace. As states are accorded sovereignty as well as immunity in governmental situations, so too, must states be responsible to terminate or mitigate harmful activity originating within or associated with its territory. Not only must states “exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of and produce adverse consequences for, other states,” the principle also requires states to take all feasible measures to end cyber activities that have adverse consequences for other states.<sup>179</sup> Once a state learns that its territory is being used for activity that is or could cause adverse consequences, it is obligated to take measures to stop the activity. Omission—not only failure to act but also failure to take effective or sufficient measures when practicable, reasonable ones are available and applicable—constitutes a violation of due diligence. Since knowledge is a basis for the rule, the IGE opined that states are not obligated to enact preventative measures for cyber activities that are unknown to the states or do not yet exist as it would be unduly burdensome and unreasonable considering the speed and attribution

---

<sup>177</sup> Schmitt, *Tallinn 2.0*. Rules 26, 71, and 20, respectively.

<sup>178</sup> Schmitt. Rule 5, 27–28.

<sup>179</sup> Schmitt. Rules 6 and 7, 30–43.

challenges of cyber operations.<sup>180</sup> However, it should be noted that the scope required by the principle is unsettled. With savvy technical, intellectual, and financial resources, developed states may be better equipped than other states to stop attacks brought to light. In addition, the measure of feasibility is dependent on circumstances. For instance, suppose the Islamic State is conducting malign cyber activities from within Jordan against France. The French are unaware of the activity, but the Jordanian General Intelligence Directorate is monitoring the activity for intelligence-gathering purposes to effectively foil a terrorist plot and further damage. In this case, delay in response outweighs immediate action. In another example, if a non-state actor or private company that owns or is in control of the platform on which malign cyber activity is being conducted refuses to cooperate with the state, unless all feasible measures consistent with international law are exhausted to obtain cooperation, the state is still in breach of the principle. The due diligence principle is not an obligation of result or ending the harmful activity, but of conduct: acting “diligently in its efforts.”<sup>181</sup>

### **3. Jurisdiction**

The principle of jurisdiction, including both territorial and extraterritorial jurisdiction in nature, applies over cyber activities and persons the same as it does other activities under international law. The general principle of jurisdiction refers to regulation of persons, objects, and activities under a state’s national law, with authority over civil, criminal, and administrative matters.<sup>182</sup> In Rule 9, the IGE stated that territorial jurisdiction applies when cyber activities originate, occur, or are completed in a state’s territory, or if the cyber activities substantially affect the state’s territory.<sup>183</sup> Whereas Rule 9 addresses activity within a state, Rule 10 addresses external activity and the scope of a state’s prescriptive jurisdiction with regard to cyber activities conducted by a state’s nationals, committed by foreign nationals against its nationals or to undermine state

---

<sup>180</sup> Schmitt, 43–47.

<sup>181</sup> Schmitt, 2.0, 49.

<sup>182</sup> Schmitt, 51.

<sup>183</sup> Schmitt, 55.

interests, or that constitutes a crime under the universality principle. Under universality, states may extend their jurisdiction over cybercrimes, which are universally recognized, regardless of the nationalities of the victims, perpetrators, or location of the offense.<sup>184</sup>

The IGE went a step further in distinguishing a state's domestic jurisdiction in light of the global interconnectedness of cyber activities and the issue of intervention via Rules 66 and 67. Based on the sovereignty principle just discussed, a state is prohibited from using cyber means to intervene in another state's internal or external affairs. What is considered to fall under internal affairs—*domaine réservé*—is broadly interpreted and constantly evolves, but the standard are those activities that fall within the prerogatives of the states and are not regulated by international law. The *domaine réservé* may narrow—although, it does not mean total control relinquishment—as more cyberspace issues become regulated under international law. External affairs are also those over which the state has prerogative, such as diplomatic and consular relations, international organization membership such as the UN or NATO, or entering into international agreements. Like sovereignty, the states, the international community, and the International Court of Justice (ICJ) regularly accept this customary international norm. Under this rule, the “interference” or “intervention” must rise by a coercive effect and only pertains to state-to-state activity unless a private organization or individual's cyber actions can be attributed to the state. The IGE agreed that the rule has two elements:

- the cyber act in question must relate to the internal or external affairs of the target state; and,
- the act must be coercive in nature and designed (note, intent) to influence or compel an outcome not only via physical use of force, but through any affirmative act designed to limit a state's freedom of choice, or to force an involuntary action or non-action of the targeted state.<sup>185</sup>

---

<sup>184</sup> Schmitt, 64–65.

<sup>185</sup> Schmitt. Rule 66, 314.

A state has a right to freedom from intervention by the UN for any matter that is within the domestic jurisdiction of the state. The rule does not allow for UN interference in cyber activities that are purely domestic (i.e., requiring a state to adopt legislation that regulates cyber activities that are *purely* domestic in character). The UN cannot prohibit China from entering its citizens' faces and social credit scores into a database and use the information to award benefits or impose punishments. However, this rule does not pertain to matters that affect international peace and security or that involve "international problems of an economic, social, cultural, or humanitarian character and ... human rights."<sup>186</sup> These two significant exemptions to Rule 67 afford the UN to intervene and opportunity for substantial involvement in cyber issues.

Effective regulation of cybercrimes demands international cooperation. States are not obligated, per Rule 13, to cooperate with other states in domestic cybercrime investigations and prosecutions—even transnational in character; however, they may be required to if they fall within the scope of a treaty or other international agreement. For example, two agreements—the League of Arab States' Arab Convention on Combatting Information Technology Offences and the Council of Europe's Convention on Cybercrime—include international cooperation provisions for mutual assistance to investigations or proceedings.<sup>187</sup>

International peace and security and cyber activities, Part III, addresses peaceful settlement, prohibition of intervention, the use of force, and collective security. Per Rule 65, "Peaceful Settlement of Disputes," and as is customary international law through multilateral and bilateral treaties, ICJ decisions, and UN resolutions, states must settle disputes by peaceful means. This rule applies to actual—and not unforeseeable, unmaterialized—international cyber disputes that endanger international peace and security. "Peaceful settlement" means solutions through arbitration, mediation, negotiation, settlements, arrangements, or any agreed-upon means.<sup>188</sup> This rule applies

---

<sup>186</sup> Schmitt, Rule 67, 325–7.

<sup>187</sup> Schmitt, 75.

<sup>188</sup> Schmitt, 303.

only to international disputes and not to internal, domestic ones. A “dispute” for purposes of this rule must rise to a “disagreement on a point of law or fact, a conflict of legal views or interests between parties ... [and] comprise a specific claim by one state that is rejected by another.”<sup>189</sup>

For this thesis, it is important to note the IGE’s stance on determining whether transnational cyber disputes between a state and non-state actor constitute international disputes for the purpose of peaceful settlement. Rule 65 is based on UN Charter Articles 2(3) and 33(1).<sup>190</sup> The majority of experts agreed that this rule only applies to disputes between states, leveraging UN Charter Article 2(4) and *Tallinn 2.0* Rule 68, which prohibits use-of-force by states against non-state actors. Any disputes with non-state actors should be settled in the spirit of the law, by peaceful means. Another notable aspect of the rule is the concept of good faith: states should not obstruct settlement through lies, delays, omissions, or any other means.<sup>191</sup> A state is not acting in good faith if, in its attempt to settle a cyber dispute involving proxy actors, the state denies any involvement when, in fact, the proxies were acting under that state’s arm.

The process of peaceful settlement occurs until there is no reasonable resolution; means to negotiate have to be exhausted. Once those efforts fail, the dispute may be elevated to the UN Security Council and General Assembly.<sup>192</sup>

### C. BUDAPEST CONVENTION

The Geneva Conventions, UN Charter, and the Council of European Convention on Cybercrime (also known as the “Budapest Convention”) are existing international

---

<sup>189</sup> Schmitt, 304.

<sup>190</sup> Article 2(3) states, “All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.” “Chapter II: Membership,” United Nations, Article 2(3), <https://www.un.org/en/sections/un-charter/chapter-i/index.html>. Article 33(1) states, “The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.” “Chapter VI: Pacific Settlement of Disputes,” United Nations, Article 33(1), <https://www.un.org/en/sections/un-charter/chapter-vi/index.html>.

<sup>191</sup> Schmitt, *Tallinn 2.0*, 308.

<sup>192</sup> United Nations, “Chapter VI: Pacific Settlement of Disputes,” Article 37(1).

instruments that could affect norms of conduct, law enforcement, investigation, security, and various agreements related to the cyber domain as long as there is cooperation with signatories. As cyber technology advances, jurisdictional boundaries may shift or remain unknown, affecting law enforcement jurisdiction to handle cybercrimes. The Budapest Convention is a step towards international cooperative governance solution for cyberspace. The treaty was opened for signature in 2001 and entered into force on January 7, 2004. It is the first international treaty on cybercrime that includes copyright infringement, child pornography, network security violations, computer-related fraud, and any other crimes committed via computer networks and the internet. Per the treaty's preamble, the fight against cybercrime requires international cooperation through a common criminal policy by the adoption of appropriate legislation by each state party to the convention.<sup>193</sup> Party states are joined by international organizations, such as the EU, International Criminal Police Organization (INTERPOL), and the UN Office on Drugs and Crime, which participate as members or observers on the Cybercrime Convention Committee.

The treaty is broken into four chapters— terms and definitions; domestic (state) level substantive law and procedural law; general principles relating to international cooperation; and, final clauses. The substantive criminal law articles address offenses and conduct—committed intentionally and without right—to include data and system interference, computer-related forgery and fraud, child pornography, copyright infringements, and corporate liability. The chapter also includes a provision averring that each state, within its adopted legislation, shall include measures that are “punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.”<sup>194</sup> The procedural law chapter addresses the scope of procedural provisions, specifically that each party shall ensure power and procedures are subject to conditions and safeguards *under each state's domestic law*, which “shall provide for the adequate protection of human

---

<sup>193</sup> “Details of Treaty No. 185, Convention on Cybercrime,” Council of Europe, November 23, 2001, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.

<sup>194</sup> “Article 13—Sanctions and Measures,” Convention on Cybercrime, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>.

rights and liberties.”<sup>195</sup> A critical element to cyber governance discussions is that of jurisdiction, which is established when the offense is committed in the state’s territory, on board a ship or aircraft registered to the state, by a state’s national, or under existing criminal jurisdiction in accordance with a state’s domestic law.<sup>196</sup>

Barnes succinctly summarized the crux of the convention in his thesis, stating that member nation-states shall adopt their legislation according to the following guidelines:

- Every network has a base level of authorized access. Entities that exceed that level of authorized access violate the law.
- Preventing access to or damaging data and/or computer networks is counterproductive to the free sharing of information and should be punished appropriately.
- Although digital devices allow the ubiquitous copying of intellectual property, they do not obliterate intellectual property protections. Nations should ensure entities respect intellectual property rights.
- Illicit images of children are inherently wrong. Nations should prosecute entities that publish and distribute such images.
- Parties that subscribe to the treaty shall cooperate with other nations to enforce these principles and share information pursuant to the appropriate legal measure to allow the extradition and prosecution of perpetrators of acts contrary to those provisions.
- Criminal liability does not attach to measures used for the protection of computers and computer networks.
- The European Committee on Crime Problems (CDPC) shall settle disputes between signatories.<sup>197</sup>

Capacity building—reinforcing criminal justice capacities for cybercrimes—has been a topic in Budapest Convention conversations. Alexander Seger avers the Budapest Convention is part of a “dynamic triangle” for cybercrime success supported by capacity-building programs. This triangle consists of the Budapest Convention, the Cybercrime Convention Committee, and the Council of Europe’s Cybercrime Programme Office (C-PROC) that was established in Bucharest, Romania, for worldwide capacity building. The

---

<sup>195</sup> “Article 14—Scope of Procedural Provisions” and “Article 15—Conditions and Safeguards,” Convention on Cybercrime, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>.

<sup>196</sup> “Section 3—Jurisdiction,” Convention on Cybercrime, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>.

<sup>197</sup> Barnes, “Implementation of Active Cyber Defense Measures by Private Entities,” 23–24.

C-PROC supports the “implementation of the Budapest Convention as well as recommendations of the Cybercrime Convention Committee; and at the same time, the experience of capacity building program [s] is fed back into the Committee and the further evolution of the Convention.”<sup>198</sup> Capacity building through bilateral cooperation is an essential ongoing process to apply cyber best practices at a global level through which the Budapest Convention provides an existing framework to leverage.

A problem that currently arises in the newer cyber domain can be seen with the Budapest Convention: the U.S. ratified the agreement but China is not a signatory, deeming the convention unsuccessful to critics.<sup>199</sup> Countries such as China have been resistant to applying current international law to cyber issues, arguing that the cyber domain is a new realm that requires different rules; however, the notion of rules of conduct and legitimate behavior continue to be discussions of interest.<sup>200</sup>

#### **D. NORTH ATLANTIC TREATY ORGANIZATION**

The North Atlantic Treaty Organization (NATO) is a military defensive alliance whose member states agree to mutual and collective defense and respond to attacks by external entities. The cornerstone of NATO is Article 5, which states that an attack of one NATO member is an attack on all of its members. Article 5 has been invoked only once after the 9/11 terrorist attacks. On September 12, 2001, Article 5 was invoked by the NATO Alliance and on October 2, 2001, NATO’s North Atlantic Council determined that Article 5 did apply to the attacks.<sup>201</sup> The Article 5 invocation demonstrated collected defense support by NATO members for the United States, taking a united stand against the terrorist attacks. As a result, NATO agreed to eight support measures including NATO military asset surveillance and air support, increased security for U.S. facilities, and readiness for

---

<sup>198</sup> Alexander Seger, “The Budapest Convention on Cybercrime: A Framework for Capacity Building,” *Global Cyber Expertise Magazine*, 2, November 2016, 30–31.

<sup>199</sup> Rollins, “U.S.-China Cyber Agreement.”

<sup>200</sup> Segal, “An Update on U.S.-China Cybersecurity Relations.”

<sup>201</sup> “Collective Defence,” NATO, accessed February 24, 2020. [https://www.nato.int/cps/en/natohq/topics\\_110496.htm](https://www.nato.int/cps/en/natohq/topics_110496.htm).

naval, air, and ground deployment support.<sup>202</sup> The Alliance currently has 29 members with membership open to “any other European state in a position to further principles of [Article 10 of the North Atlantic Treaty] and to contribute to the security of the North Atlantic area.”<sup>203</sup> Within NATO’s organizational structure, the parties with the most influence and responsibility for advancing the international cyber governance agenda on the Civilian Structure would be the NATO Secretary General, Emerging Security Challenges Division, Defence Policy and Planning Division, Joint Intelligence, and Security Division; the Allied Command Transformation (ACT) and Allied Command Operations (ACO) influence the Military Structure. The Secretary General is NATO’s top international civil servant, head of NATO’s international organizational staff, and chief spokesperson responsible for “steering the process of consultation and decision-making in the Alliance and ensuring that decisions are implemented.”<sup>204</sup> As cyber threats evolve, the frequency and complexity increases by which they impact Alliance networks. As a result, cyber is a NATO core task of its collective defense to enhance cyber resiliency and security across the Alliance.

The 2014 NATO Wales Summit reached a consensus that cyberspace should be governed by international law. However, no additional action has been pursued. In its December 2019 London Declaration, NATO recognized the rising strategic threats and challenges to transatlantic cyber security and rules-based international order emanating from states such as Russia, China, and non-state actors including terrorists, averring cooperative progress with the UN and NATO-EU relations.<sup>205</sup> Improved collaborative

---

<sup>202</sup> NATO.

<sup>203</sup> “NATO Enlargement,” NATO, accessed January 15, 2020, <https://www.nato.int/nato-welcome/index.html>; the 12 founding members of the Alliance: Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom and the United States. The other member countries are: Greece and Turkey (1952), Germany (1955), Spain (1982), the Czech Republic, Hungary and Poland (1999), Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia and Slovenia (2004), Albania and Croatia (2009), and Montenegro (2017). “Member Countries,” NATO, accessed January 15, 2020, [https://www.nato.int/cps/en/natolive/topics\\_52044.htm](https://www.nato.int/cps/en/natolive/topics_52044.htm).

<sup>204</sup> “NATO International Staff,” NATO, accessed January 15, 2020, [https://www.nato.int/cps/en/natohq/who\\_is\\_who.htm](https://www.nato.int/cps/en/natohq/who_is_who.htm).

<sup>205</sup> “London Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council,” NATO, Press Release 115, December 4, 2019, [https://www.nato.int/cps/en/natohq/official\\_texts\\_171584.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_171584.htm?selectedLocale=en).

efforts between intelligence and Centres of Excellence will support the international regulatory evolution and development of a governance framework.

Since September 2014, NATO has made cyber defense, resilience, training, and education main foci and core tasks of its collective defense through its NATO Policy on Cyber Defence (updated and endorsed in February 2017), its 2016 Cyber Defence Pledge, recognition of cyberspace as a military domain, and through its affirmation that existing international laws apply to state activity in the cyber landscape during peacetime and conflict. However, NATO has not been able to sufficiently unravel the gray area containing *how* the international laws apply or how they apply to non-state and proxy-state actors. The Alliance has intensified its commitment to preparedness, mitigation, and recovery from cyberattacks through enhanced information sharing with partners and industry through vehicles such as the NATO Industry Cyber Partnership, the NATO-EU Technical Arrangement on Cyber Defence (February 2016), NATO Cyber Rapid Reaction teams, and a new Cyberspace Operations Centre as part of its Command Structure.<sup>206</sup> Senior NATO and EU officials met in Brussels on December 17, 2019, to discuss enhanced security efforts and cyber-security initiatives as a strategic issue of common interest to promote stability between nation-states.<sup>207</sup> The following cyber initiatives and efforts will play crucial roles in non-state cyber governance:

- **NATO Industry Cyber Partnership (NICP):** This partnership recognized that industry is a key component in the cyber domain, whose capabilities and cooperation are crucial to NATO's and allies' Enhanced Cyber Defence Policy's objectives, including information sharing, prevention, mitigation, and response to cyber threats and vulnerabilities.<sup>208</sup>

---

<sup>206</sup>“Cyber Defence,” NATO, September 6, 2019, [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm).

<sup>207</sup> “NATO, European Union Experts Review Cyber Defence Cooperation,” NATO, December 17, 2019, [https://www.nato.int/cps/en/natohq/news\\_172157.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/news_172157.htm?selectedLocale=en).

<sup>208</sup> “NATO Industry Cyber Partnership (NICP),” NATO Communications and Information Agency, accessed January 12, 2020, <https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx>.

- **2016 Cyber Defense Pledge:** Each NATO member and ally agreed to make cyber defense a priority, separately and collectively as part of hybrid campaigns to “improve resiliency” and respond to cyberattacks.<sup>209</sup>
- **NATO Computer Incident Response Capability (NCIRC):** NCIRC, which is a subset of the NATO Communications and Information Agency (NCI Agency) Cyber Security (CS) Service Line (SL), provides cyber specialist services—such as development of new technology and innovation in CIS Security, Cyber Defense, Information Assurance, Computer Security & Communications Security—for the prevention, detection, response, and recovery from cyber security incidents.<sup>210</sup>
- **Memorandum of Understanding on Cyber Defence:** This MOU between NATO and 28 Allied cyber defense authorities was developed in 2015.
- **NATO Defence Planning Process (NDPP):** The NDPP is a five-step process—establish political guidance, determine requirements, apportion requirements and set targets, facilitate implementation, and review results—focused on military and non-military cyber capabilities interoperability and standardization.<sup>211</sup> The NDPP’s aim is to provide NATO allies a common framework to harmonize defense activities utilizing cyber capabilities in the most effective ways without compromising nation-state sovereignty.<sup>212</sup> Fourteen planning domains are involved in minimizing duplicity and

---

<sup>209</sup> NATO, “Cyber Defence.”

<sup>210</sup> “Cyber Security,” NATO Communications and Information Agency, accessed January 12, 2020, <https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx>.

<sup>211</sup> Dieter Schmaglowski, “The NATO Defence Planning Process (NDPP): An Overview,” NATO Standardization Office, October 30, 2018, [https://www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/2018%20International%20Standardization%20Workshop/20181030--Item3-NDPPOverview-IntlStdznWorkshop\\_Schmaglowski.pdf?ver=2018-11-06-151624-033](https://www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/2018%20International%20Standardization%20Workshop/20181030--Item3-NDPPOverview-IntlStdznWorkshop_Schmaglowski.pdf?ver=2018-11-06-151624-033); NATO, “NATO Defence Planning Process,” accessed March 22, 2020, [https://www.nato.int/cps/en/natohq/topics\\_49202.htm](https://www.nato.int/cps/en/natohq/topics_49202.htm).

<sup>212</sup> “NATO Defence Planning Process,” NATO, accessed March 22, 2020, [https://www.nato.int/cps/en/natohq/topics\\_49202.htm](https://www.nato.int/cps/en/natohq/topics_49202.htm).

maximizing cohesion in capability development.<sup>213</sup> Allies provide data every two years to update NDPP plans and policies.

- **Technical Arrangement on Cyber Defence:** This February 10, 2016, agreement between the NCIRC and the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU), provides a “framework for exchanging information and sharing best practices between emergency response teams” to augment cyber defense capabilities.<sup>214</sup> This arrangement is part of the collaborative work NATO does with the EU, UN, Council of Europe, and the Organization for Security and Cooperation in Europe.<sup>215</sup>
- **NATO Cyber Education Institutions:** These institutions comprise the Communications and Information Systems School (Latina, Italy), NATO School (Oberammergau, Germany), NATO Defense College (Rome, Italy), and NATO CCDCOE. A critical component of NATO’s cyber education is hosting recurring exercises, such as the annual Cyber Coalition Exercise, which integrates cyber defense and security elements into Alliance training.<sup>216</sup>
- **NATO Cooperative Cyber Defence Centre of Excellence:** The NATO CCDCOE is a NATO-accredited cyber research and training facility—not part of the NATO Command Structure—that offers expertise on cyber defense and security issues.<sup>217</sup> Distinguishing between peacetime and wartime is important, as both areas are still heavily being explored and have many gaps. The *Tallinn Manual* was developed between 2009 and 2012 to

---

<sup>213</sup> NATO, “NATO Defence Planning Process.”

<sup>214</sup> NATO, “NATO, European Union Experts Review Cyber Defence Cooperation.”

<sup>215</sup> “NATO Cyber Defence,” NATO, Fact Sheet, July 2016, [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2016\\_07/20160627\\_1607-factsheet-cyber-defence-eng.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf).

<sup>216</sup> NATO.

<sup>217</sup> NATO.

make rules about certain aspects of international law—*jus ad bellum*, *jus in bello*, and international humanitarian law—that apply to cyber conflicts and cyber warfare.<sup>218</sup> *Tallinn Manual 2.0*, published in 2017, expanded on the original edition *Tallinn Manual* with analysis of cyber incidents that fall below the threshold for use of force as a resource for peacetime rather than cyber warfare/armed conflict. Both manuals resulted from the academic, non-binding studies and discussions by an independent group of international renowned legal experts at the behest of the NATO CCDCOE in Tallinn, Estonia. The CCDCOE is a NATO-accredited group of experts from 25 countries who support NATO-member nations with cyber technology and legal strategy, research, and training to “address the growing relevance of potential threats within the cyber domain.”<sup>219</sup> The CCDCOE is *not* directly funded by nor part of the command structure of NATO; its role is to support the NATO Alliance through its specialized cyber functional area. The non-binding *Tallinn Manuals* follow the paths of other non-binding productions such as the International Institute of Humanitarian Law’s *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* and the Harvard Program on Humanitarian Policy and Conflict Research’s *Manual on International Law Applicable to Air and Missile Warfare*.

## E. THE UNITED NATIONS

The UN Charter, signed on June 26, 1945, and in effect since October 24, 1945, provides principles and obligations for its members and non-members as applicable for maintenance of international peace and security. Article 106 reinforces that member parties to the Four-Nation Declaration (the United States, the United Kingdom, the former Soviet

---

<sup>218</sup> The *Tallinn Manual* was published in April 2013 by Cambridge University Press.

<sup>219</sup> Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. “About Us,” CCDCOE, <https://ccdcoe.org/about-us/>.

Union, and China), which was signed at the Moscow Conference on October 30, 1943, and France, must consult with one another as is necessary to “maintaining international peace and security.”<sup>220</sup>

The UN Group of Governmental Experts on Developments in Field of Information and Telecommunications in the Context of International Security recognized the relevance of the UN Charter’s prohibition on use of force in cyberspace; however, the group requires further studies to understand the application of the prohibition as well as the norms of international law.<sup>221</sup>

### **1. UN Security Council**

The UN Security Council is the main UN body responsible for maintaining international peace and security. The council consists of 15 members, each with one representative/one vote allocated to it. The United States, the United Kingdom, Russia, China, and France are the five permanent members (known as the P5) that have UN resolution veto power and 10 members are elected by a two-thirds vote of the General Assembly for two-year nonconsecutive terms but not afforded resolution veto power.<sup>222</sup> In terms of the veto power, Russia has used it the most, followed by the United States, and then, China. Any UN but non-council member may participate in discussions for issues that affect that UN member nation.<sup>223</sup> The Security Council has a right to mandate and authorize measures, should it find any cyber activity it deems an act of aggression, threat, or breach to international peace and security. Per chapter 7 of the UN Charter, once the council adopts a binding resolution—for example, deny access to cyber communications

---

<sup>220</sup> “Chapter XVII: Transitional Security Arrangements,” United Nations, Article 106, <https://www.un.org/en/sections/un-charter/chapter-xvii-0/index.html>.

<sup>221</sup> Group of Governmental Experts, “Developments in the Field of Information and Telecommunications in the Context of International Security,” United Nations General Assembly, Sixty-Eighth Session, (2013), <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf>.

<sup>222</sup> “Chapter V: The Security Council,” United Nations, accessed January 15, 2020, <https://www.un.org/en/sections/un-charter/chapter-v/index.html>.

<sup>223</sup> United Nations.

from one state—all states must adopt and adhere to its decisions.<sup>224</sup> A state’s compliance with such a mandate will not be in violation of the rule against intervention.<sup>225</sup>

The UN Secretary General sponsors the annual Internet Governance Forum in accordance with the mandate set out in the “Tunis Agenda for the Information Society,” a 2005 publication from the World Summit on the Information Society. This forum focuses around the consensus that global internet governance should be a multilateral and transparent process, a core focus for all nation governments, international organizations, the private sector, and individual citizens to provide a stable and secure cyberspace. This consensus is further support for the approach taken in this paper.

A main limitation of the UN Security Council is the membership of China and Russia as permanent seats. These two P5 countries skillfully use procedural rules and tactics to sway the UN in their favor and promote their agenda, even if the result can have dire consequences. An example is the recent Russia-supported UN cybercrime resolution, “Countering the Use of Information and Communications Technologies for Criminal Purposes” that was passed November 18, 2019.

## **2. The International Court of Justice**

The ICJ is the principal judicial structure of the United Nations per Article 92 of the UN Charter and based on the Statute of the Permanent Court of International Justice. UN Members are *ipso facto* parties to the ICJ and non-members may, by determination and recommendation by the General Assembly through the Security Council, become a party to the ICJ.<sup>226</sup> Members are not required to take their cases to the ICJ. They are authorized to use other agreements, whether in existence, planned, or tribunals; however, if they choose to bring a case to the ICJ, the parties must comply with the decision, with any

---

<sup>224</sup> “Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression,” United Nations, accessed March 22, 2020, <https://www.un.org/en/sections/un-charter/chapter-vii/index.html>.

<sup>225</sup> Schmitt, *Tallinn 2.0*. Rule 67, 325–327.

<sup>226</sup> “Chapter XIV: The International Court of Justice,” United Nations, Article 93, <https://www.un.org/en/sections/un-charter/chapter-xiv/index.html>.

recourse for party noncompliance elevated to the Security Council for judgment.<sup>227</sup> An important aspect of the ICJ to consider in the international governance analysis is the court's ability to provide advisory opinions on *any* legal question not only to the General Assembly or Security Council but also to other UN bodies or specialized agencies.<sup>228</sup>

## **F. CONCLUSION**

Chapter III provided an overview of the critical cyber concepts and legal principles embodied in interpretations of ROE, the Budapest Convention, and through restatements of law in *Tallinn 2.0*. The chapter concluded with an overview of the applicable cyber functions provided by the UN and NATO. It is important for the reader to understand these concepts and organizational contributions as integral aspects of cyber governance, peace, and security. Chapter III provided an essential knowledge foundation leading into Chapter IV's regulatory mechanism analysis.

---

<sup>227</sup> United Nations, Articles 94, 95.

<sup>228</sup> United Nations, Article 96.

THIS PAGE INTENTIONALLY LEFT BLANK

#### **IV. IS NATO CCDCOE THE RIGHT ENTITY TO ARBITRATE CONFLICT IN THE CYBER DOMAIN?**

The NATO CCDCOE, leveraging the Budapest Convention framework, is not the correct regulatory entity for international governance of non-state actors—or any actors—in the cyber domain. One governing entity is not a sufficient approach for dispute resolution. The majority of today’s malicious cyber activities consist of spreading false information, stealing personal data, or breaching government systems. These actions pose a direct threat to the public and private sectors, nation-states, and the international community. Cyberattacks by non-state actors have evolved with the speed of technology development, leaving governments powerless to address the threat due to a lack of legal options to regulate non-state actors. To adequately address the threat, the international community must form legally binding mechanisms to pursue non-state actors similar to the way the world rethought terrorism and the threats posed to national security interests after 9/11. Although ambiguity surrounds the application of international law in cyberspace, collective action founded in legal principles that could provide cyber-victim recourse options should be a priority of the international community.

A one-stop shop is a cyber-governance paradise, the ideal destination. Unfortunately, the current—and indeterminate future—landscape is too complex an environment to be solved with the press of an “easy button.” For example, if the United States decided to leverage the full capabilities of the government to include intelligence, military and law enforcement, what risks does the United States run in pursuing, exposing, and responding to an attack? Is the United States willing to expose its capabilities to the public in pursuit of the perpetrators of the attack? Is it worth exposing sensitive collection capabilities or embarrassing an ally who may have inadvertently been used as an accomplice? These were the challenges that the U.S. government faced in response to the 2016 election interference. What are a private corporation’s financial risks if it reveals publicly it has been a victim of cybercrime? Indeed, each situation will force difficult challenges for the involved victims and nation-states attempting to combat the threat, which is why the issue must be elevated and addressed within the international community. As

our understanding of the cyberspace matures, standards and norms backstopped by international law should also mature and evolve to address the regulatory requirements.

This thesis centers on Barnes's recommended future course of study to elevate the NATO CCDCOE to a formal arbitrating body using the Budapest Convention as a framework. Barnes's designation of the CCDCOE is based on the its history with cybersecurity; specifically, its IGE that interpreted and restated international law—captured in the *Tallinn Manuals*—as applied to the cyber domain. Barnes's argument is that by empowering the CCDCOE to mitigate cyber disputes, information sharing will be easier while at the same time making it harder for “enemies to remain anonymous.”<sup>229</sup> In addition to stating that the U.S. Executive Branch should work with international partners to determine the best active cyber defense measures in accordance with ACDA, he avers the branch also has an integral role in modifying the NATO charter to enable and allow for the CCDCOE to continue its *Tallinn 2.0* legal analysis and to develop into a governance body responsible for dispute mitigation and resolution.<sup>230</sup>

Barnes's recommendation is flawed for two reasons: the CCDCOE is not the appropriate regulatory mechanism and the framework should include *Tallinn Manual 2.0* restatements of law in addition to the Budapest Convention. The CCDCOE is comprised of the expertise necessary to weigh on disputes concerning conflicts and violations of international law; however, a group composed of attorneys, academics, and cyber professionals who developed *nonbinding* manuals will be perceived as having weak authority to resolve disputes. Even if a convention is created to statutorily elevate the Centre CCDCOE to an arbitrating body, cyberspace is a complex domain that requires more than a simple, one-body entity as a regulatory solution. The Budapest Convention is an ideal framework for addressing cybercrime both unilaterally and bilaterally due to its extradition principles and procedures. However, its effectiveness will be lost if it is used alone and relied on as the sole framework to address international governance of non-state actors.

---

<sup>229</sup> Barnes, “Implementation of Active Cyber Defense Measures by Private Entities,” 57.

<sup>230</sup> Barnes, 53.

Barnes drives the discussion in a promising direction: the NATO CCDCOE expertise and the Budapest Convention should be leveraged in the development of a regulatory mechanism but, at present, it needs to be a multilateral, multipronged approach. This approach should consider the Paris Climate Agreement Model and *Tallinn Manual 2.0* with the Budapest Convention as a framework, and encompass multilateral processes through the UN, NATO, INTERPOL, and unilateral state processes (e.g., United States only).

#### **A. THE PARIS CLIMATE AGREEMENT MODEL**

One of the main challenges in developing an international cyber governing mechanism is obtaining consensus among the cybersphere of parties. The international community should follow the recent Paris Climate Agreement (also referred to as “Paris Agreement”) as a model for success in garnering support for a major global initiative. The agreement, adopted in 2015 and made effective November 2016, was designed to improve on and replace the Kyoto Protocol, a 2005 treaty to reduce greenhouse gas emissions. The Paris Agreement—part of the UN Framework Convention on Climate Change (UNFCCC)—is a landmark treaty. As of February 2020, 189 (including the EU) out of the 197 parties have ratified to the treaty.<sup>231</sup> Only eight countries in the world have signed but not yet ratified: Angola, Eritrea, Iran, Iraq, Libya, South Sudan, Turkey, and Yemen.<sup>232</sup> The UNFCCC serves as the “foundation for intergovernmental action to combat climate change and its impacts on humanity and ecosystems” with the Paris Agreement building upon the convention to achieve a common goal to reduce global temperature rise and bring temperatures below pre-industrial times.<sup>233</sup>

---

<sup>231</sup> “2020 United Nations Framework on Climate Change, Paris Agreement-Status of Ratification,” United Nations, accessed February 28, 2020, <https://unfccc.int/process/the-paris-agreement/status-of-ratification>.

<sup>232</sup> “Chapter XXVII, Charter of the United Nations and Statute of the International Court of Justice: Paris Agreement,” United Nations, December 12, 2015, [https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=XXVII-7-d&chapter=27&clang=\\_en](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVII-7-d&chapter=27&clang=_en)

<sup>233</sup> “The Paris Agreement,” UNFCCC, accessed February 28, 2020, <https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement>.

To effectively follow this model, global leaders would need to collectively agree that characteristic malign cyber activities are driven by state, proxy, or non-state actors; those activities are a threat to the cyber environment and all of humanity, and that international action is required to halt it. In addition, a clear framework must be created for all countries to make commitments to reduce malign cyber activities that occur within or are associated with their state, according to the legal framework that follows, to include non-state activities. Finally, the parties to a similar cyber model would need to make a commitment to strengthen international governance of cyberspace over time.

Key Paris Agreement takeaways that should be applied to a cyber governance model include:

- **A clear, well-defined technology and legal framework.**
- **Enhanced capacity building framework supporting action by developing and vulnerable countries.** This takeaway supports the issue raised in Chapter III, Section B.2, that undeveloped states may suffer more attacks because they are not well equipped or they may not be in compliance with regulation because they do not have the financial, personnel, or technological resources to do so.
- **Enhanced transparency of action and support through a more robust transparency framework.** The heart of the Paris Agreement is its reliable, transparent, and comprehensive reporting requirements to achieve its goals. All parties must communicate on their adaptation, implementation, and mitigation efforts through nationally determined contributions (NDC) and an assessment every five years to evaluate the collective progress toward achieving the agreement's purpose.<sup>234</sup> Each party agrees to regularly "prepare, communicate, and maintain successive nationally determined contributions (NDCs) that it intends to achieve," with a plan tailored to the

---

<sup>234</sup> "Transparency and Reporting," UNFCCC, accessed February 28, 2020, <https://unfccc.int/process-and-meetings/transparency-and-reporting/the-big-picture/what-is-transparency-and-reporting>.

country's current capabilities and existing domestic conditions to ensure adequate compliance and forward-moving direction toward the agreement's objectives.<sup>235</sup> In addition, an Ad Hoc Working Group on the Paris Agreement (APA) was established at the same time as the agreement to provide guidance as well as share general expectations and understanding of the work required by the parties to the Paris Agreement.<sup>236</sup> Leveraging this model, a similar Ad Hoc Working Group on Cyber Governance should be established at the same time, or before, a governance framework and process is developed. The Paris Agreement demonstrates that global warming can only be mitigated with global action. Cyber governance requires a carbon copy response by establishing legally binding measures in a comprehensive treaty that includes monitoring, reporting, and assessment requirements. Such a cyber treaty will not be the ultimate answer to cyberspace regulation; however, there needs to be a solid floor before the cyber governance ceiling can be reached.

## **B. FRAMEWORK FOR DEVELOPING LEGAL STANDARDS**

An effective framework for international governance during peacetime of non-state actors requires the Budapest Convention and the *Tallinn Manual 2.0* restatements of the law, in addition to the manual's commentary. The analysis in this thesis demonstrates that Barnes is correct in his assertion that the Budapest Convention should be leveraged. The convention's framework should be used for all criminal activity and expanded as necessary as the cyberspace evolves. As mentioned in Chapter III, Section C, the convention allows for amendments as well as for additional parties. The most recent amendment, the 2006 Additional Protocol to the Convention on Cybercrime, was created to extend the Budapest

---

<sup>235</sup> "Nationally Determined Contributions (NDCs)," UNFCCC, accessed February 28, 2020, <https://unfccc.int/process-and-meetings/the-paris-agreement/nationally-determined-contributions-ndcs>.

<sup>236</sup> "Ad Hoc Working Group of the Paris Agreement (APA)," UNFCCC, accessed February 28, 2020, <https://unfccc.int/process/bodies/subsidiary-bodies/apa>.

Convention's scope through criminalization of racist and xenophobic cyber activities and threats using computer systems.<sup>237</sup>

The convention also has a built-in working group to provide guidance, assessment, and strategic direction as well as appropriate amendments. Through Article 46, the Cybercrime Convention Committee is the quality control mechanism through which parties to the convention “consult periodically ... with a view to facilitating ... the effective use and implementation of the Convention, the exchange of information, and the consideration of possible supplementation or amendment of the Convention.”<sup>238</sup> As cyberspace is defined, the Budapest Convention should be amended to include a wider range of cybercriminal and other non-state cyber activities.

In addition to the convention, the *Tallinn Manual 2.0* should be a focal component of the framework. In consideration of cyberspace's rapid evolution and key players, the manual's restatements of law should be expanded to include non-state activity, either through attribution or forensic analysis, to associate them with a state, for international law application. The principles of sovereignty, due diligence, and jurisdiction will be a foundation to the framework. As the restatements are translated into binding law, the principle of sovereignty—and thereby, attribution—will be a main factor in non-state governance. It is clear that sovereignty applies only to states. However, *Tallinn 2.0* Rules 1, 2, and 3 provide wiggle room for internal and external sovereignty over non-state actors based on the person's location or infrastructure used in the cyber activity. A state could also be held in violation of a non-state activity if it did not terminate or mitigate the harmful activity within its jurisdiction or associated with its territory, per the international law principle of due diligence. The manual's restatements will not provide a blanket solution for a binding legal framework because, in its current state, the manual is comprised of non-binding expert opinions. However, the restatements provide a comprehensive guide to replicate or refine existing legal principles understood by the global community.

---

<sup>237</sup> Council of Europe, “Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems,” ETS No. 89, January 3, 2006, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>.

<sup>238</sup> “T-CY Work Plan for the Period 1 January 2018 – 31 December 2019,” Council of Europe, November 27, 2018, <https://rm.coe.int/t-cy-2018-27-tcy-workplan-v6adopted/16808feb6c>.

### C. MULTI-PRONGED APPROACH FOR CYBER GOVERNANCE

Numerous stakeholders influence cyber strategies in the United States and internationally. A one-system regulatory mechanism will not be an effective measure for international cyber governance. Rather, a multi-pronged, multilateral, and unified approach—with concession by a majority of the international cyber community—is preferred to achieve the greatest success.<sup>239</sup> Cyber governance success would be measured on the ability to hold a cyber actor(s) responsible for malign activity, whether it is an individual, transnational organization, or—at the highest level—a nation-state. See Figure 11.

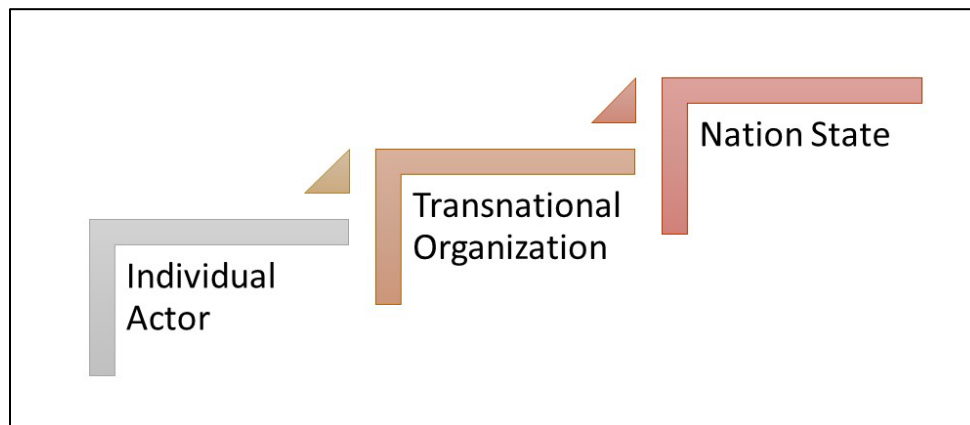


Figure 11. Steps in Accountability for Malign Activity

The purpose of this recommended approach is not to provide the ultimate solution; it is to provide the international community with a course of action to consider in developing a regulatory mechanism. The United States will benefit most from driving the discussions and leading the process development. This process requires classification on some level, whether known outright or through forensic analysis, to attribute the activity to a non-state, proxy, or nation-state actor. Following in the path of the Paris Agreement, the approach should begin with defining cyberspace as it applies to non-state actors and garnering global support through a clear, well-defined framework to design a treaty. Once

---

<sup>239</sup> It is well understood that international governance will never be purely unified, as there will always be states—adversaries to Western countries, for example—who disagree with regulatory measures that do not support their policies that are information-restrictive or limit cyberspace access to its civilians.

signatories and ratification take place, the multi-pronged approach will include NATO, INTERPOL, and unilateral processes.

Figure 12 proposes the multipronged approach and is discussed further in this chapter.

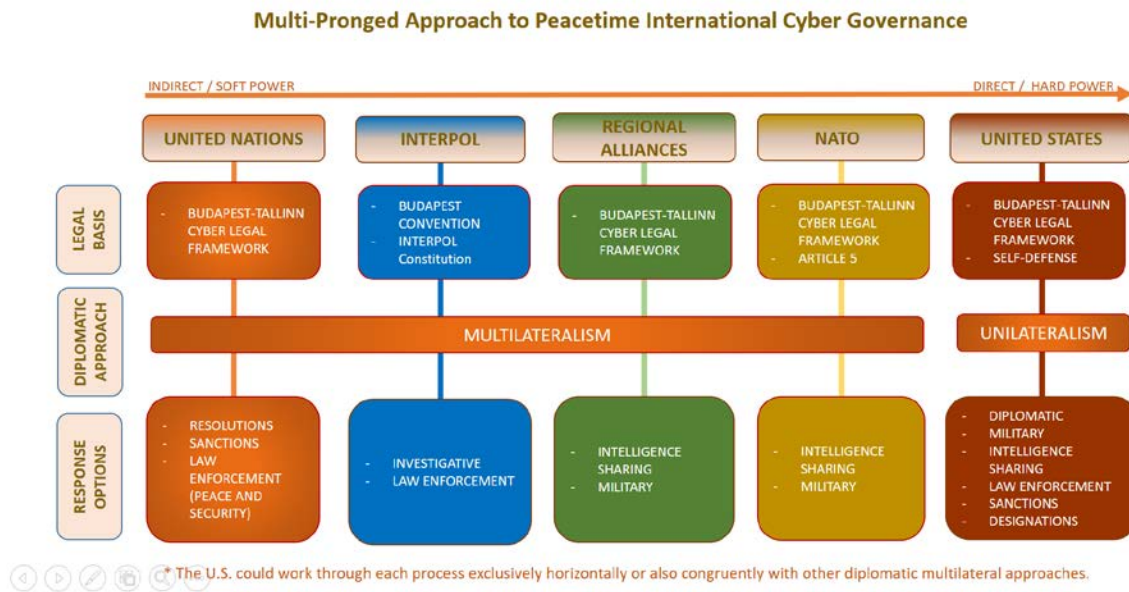


Figure 12. Recommended Governance Approach

## 1. Defining the Space via the UN

The UN should be charged with the challenge of defining cyberspace and establishing binding legal documents for the multilateral, multi-pronged approach by leveraging the international community's cyber experts and modeling existing treaties. When defining the space, the UN should present a course of action referencing the Outer Space Treaty within the Budapest-Tallinn- cyber framework. The Outer Space Treaty model is based on a non-armament treaty for international cooperation to maintain a peaceful outer space to limit damage from self-serving exploitation of the new domain. The 1967 "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies" seeks to protect space

use and exploration through demilitarization for the benefit of all humanity, in the interests of all countries, in accordance with international law.<sup>240</sup> Per Article VI, the Outer Space Treaty mandates that state parties to the treaty have the *international* responsibility for all activities that occur in outer space (including the moon and other celestial bodies), whether conducted by *governmental or non-governmental entities*.<sup>241</sup> Defining a cyberspace governance process in a similar manner to account for non-state actors will be beneficial in addressing a major area of cyber activities. The UN should provide clarity regarding information flows and determining the correct pathway or prong(s) to pursue against non-state actors, which may be case dependent as governance matures. The process should be made enforceable by a treaty based on the recommended Budapest-Tallinn legal framework, models, and multi-pronged approach, as discussed. The treaty should be flexible, allowing for amendments that account for various types of non-state and other cyber activities as the cyberspace evolves.

## **2. Diplomatic Approaches**

There are two types of diplomatic approaches to consider when developing the multi-pronged methodology: multilateralism and unilateralism. Simply put, multilateralism is acting in cooperation with other states or international organizations; unilateralism is a state acting on its own without international support.<sup>242</sup> Unilateralism often has negative connotations in international relations when states act with disregard for other states. However, in this multi-pronged approach, unilateralism is used positively regarding self-defense. The Budapest Convention also affords unilateral action for cybercrimes. As mentioned throughout this paper, international cooperation is necessary for cyber governance success. Which multilateral mechanism is used will depend on the

---

<sup>240</sup> “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Article VI,” Department of State, 1967, <https://2009-2017.state.gov/t/isn/5181.htm>.

<sup>241</sup> Department of State.

<sup>242</sup> Joseph S. Nye, Jr., “Unilateralism vs. Multilateralism,” *International Herald Tribune*, June 13, 2012, <https://www.globalpolicy.org/component/content/article/199/41054.html>.

type of activity and process defined by the UN using the Budapest-Tallinn legal framework.

### **3. Response Capabilities in a Defined Cyber Environment**

Regional alliances, NATO, and INTERPOL have capabilities that aid in cyber conflict resolution, mitigation, and cyber incident responses. These unions and organizations should be involved in cyber governance processes to ensure a robust, comprehensive approach to maintaining international cyber peace and security.

#### ***a. Regional Alliances***

Regional alliances are political and economic unions based within geographic areas, to include the EU, the African Union (AU), and the Gulf Cooperation Council (GCC). The EU is the most recognizable alliance, currently consisting of 27 member countries and exists to “enhance economic, social and territorial cohesion and solidarity among EU countries” through trade, diplomacy, security, and technological progress.<sup>243</sup> The AU, created in 2002, is a regional organization of 55 member countries that focuses on increased cooperation between African nations for economic growth through conflict resolution, crisis management, and promoting peace and security.<sup>244</sup> Its constitutive aims include international cooperation, promoting peace, security, and stability on the continent, and establishing a role in international negotiations.<sup>245</sup> The GCC is a regional effort that was established in 1981 with six Middle Eastern member states—Saudi Arabia, Kuwait, the United Arab Emirates, Qatar, Bahrain, and Oman—to develop and maintain coordination, cooperation, and technological progress for Arab regional unity.<sup>246</sup> Critical cyber governance responses at the regional alliance prong could be intelligence sharing and military response, whether it is a standalone force or leveraging

---

<sup>243</sup> “The EU in Brief,” European Union, accessed February 29, 2020, [https://europa.eu/european-union/about-eu/eu-in-brief\\_en](https://europa.eu/european-union/about-eu/eu-in-brief_en).

<sup>244</sup> “In a Nutshell,” African Union, accessed February 29, 2020, <https://au.int/en/au-nutshell>.

<sup>245</sup> “Overview,” African Union, accessed February 29, 2020, <https://au.int/en/overview>.

<sup>246</sup> “About GCC,” Gulf Corporation Council, accessed February 29, 2020, <https://www.gcc-sg.org/en-us/AboutGCC/Pages/StartingPointsAndGoals.aspx>.

member states' capabilities. The EU, for instance, does not have its own military force but instead relies on the military capabilities of other member states. The African Standby Force, under the AU's direction, is comprised of military, police, and civilians to respond to international and continental crises.<sup>247</sup> The GCC created its own military bridge, the Peninsular Shield Forces, which was disbanded in 2006.<sup>248</sup>

The type of force would depend on the action and how the space is defined by the UN. Including regional alliances as a facet of a multipronged approach is important because it ensures mutual interests and benefits of the world's key players, regional relationships, and emerging powers all have a role in international cooperation and governance.

#### **b. INTERPOL**

INTERPOL provides a criminal cooperation and investigative support mechanism that should be leveraged by nation-states as part of a multi-pronged response to non-state cyber incidents. INTERPOL is an intergovernmental organization with 194 member countries that connects and coordinates with international police networks through data sharing and technical and operational support.<sup>249</sup> INTERPOL could have a key role in governance of non-state cyber actors, specifically with pursuing the detention and transfer of custody of cybercriminals and terrorists.<sup>250</sup> INTERPOL aids in terrorism cases through intelligence sharing, providing data that identifies suspects and prevents terrorist travel, and assisting with financial and social media analyses. INTERPOL has regional and international strategic partnerships to aid in combatting terrorism.

---

<sup>247</sup> "African Standby Force (ASF)," African Union, accessed February 29, 2020, <https://www.peaceau.org/en/page/82-african-standby-force-asf-amani-africa-1>.

<sup>248</sup> "Gulf Cooperation Military Guide," Global Security, accessed February 29, 2020, <https://www.globalsecurity.org/military/world/gulf/index.html>.

<sup>249</sup> "What is INTERPOL?" INTERPOL, accessed February 29, 2020, <https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>.

<sup>250</sup> INTERPOL, *The Constitution of the ICPO-INTERPOL*, Articles 2, 3, 9 (Vienna - 1956), Amended 2017. <https://www.interpol.int/content/download/590/file/Constitution%20of%20the%20ICPO-INTERPOL-EN.pdf>.

The organization also provides investigative support for cybercrime—“pure cybercrime”—which is referred to as “crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user... [and] cyber-enabled,” traditional crimes such as theft, fraud, and illegal gambling that are accomplished via the internet.<sup>251</sup> INTERPOL’s cyber operations, investigative support, training, and partnerships complement the international law enforcement community. The investigative and intelligence support element that INTERPOL could provide to cybercrime and cyberterrorism is an integral component of a multi-pronged governance approach, especially regarding non-state cyber activities.

*c. NATO*

NATO provides a collective defense response option, including military and intelligence sharing. Invoking Article 5 should be an option if a cyberattack is conducted on a NATO alliance member and thereby treated as an attack on all members of the alliance. If, based on the defined cyberspace and Budapest-Tallinn legal framework, it is determined that Article 5 applies to cyber activities, then it could also be invoked against non-state cyber actions. The only time Article 5 was invoked was after the 9/11 terrorist (non-state actors) attacks. Based on the application of the article to this event, a cyberattack against one could be deemed an attack against all and appropriate measures would follow per NATO’s collective defense responses. It is imperative that the space is clearly defined in order to determine the threshold at which Article 5 can be invoked in the cybersphere. It will be a case-by-case determination, so clarity is required to avoid reckless, retaliatory cyber behavior by alliance members.

In addition to Article 5, NATO offers several other platforms that can be leveraged based on the non-state cyber activity conducted. The international cyber governance approach can include NATO’s strategic initiatives discussed in Chapter III, Section D: NATO Industry Cyber Partnership (NICP), NCIRC, and its Technical

---

<sup>251</sup> “Cybercrime,” INTERPOL, accessed February 29, 2020, <https://www.interpol.int/en/Crimes/Cybercrime>.

Arrangement on Cyber Defence. These initiatives provide mechanisms for detection, response, and recovery from cyber incidents. In addition, NATO can provide legal and technical cyber expertise to the governance structure through its Cyber Education Institutions and the NATO CCDCOE.

Although the CCDCOE should not be the sole governing body, it should still play an important role in cyber governance due to its ties with the *Tallinn Manuals* and its legal expertise. The CCDCOE specializes in cyber issues and, as subject matter experts in the cyber field, distributes its expertise through consultation, doctrine, training, seminars, best practices and lessons learned. In addition to supporting NATO and partner countries with its in-depth knowledge, the CCDCOE helps to expand interoperability and increase capabilities for augmentation in the cyber domain. CCDCOE membership is open to all NATO nations and welcomes contributing participants, including non-NATO nations, academic and research institutions, and corporations.

#### **d. United States**

As previously mentioned, the United States has a unilateral response option in addition to the multilateral response options. If the United States is acting in self-defense to a non-state cyber action, it can resort to unilateralism by using the Budapest-Tallinn legal framework or its own domestic legislation. Examples of this type of response include diplomacy, military action, intelligence sharing and operations, law enforcement and investigations, and sanctions. In addition, the United States can designate terrorist organizations, which would open up additional response options such as prosecution of U.S. persons for providing terrorist support. While the international community develops and defines cyberspace regulatory mechanisms, the United States should address issues unilaterally if it is not only in the nation's best interests but also in the whole-of-cyberspace's interests to disrupt, mitigate, or remedy a malign non-state cyber activity.

The analysis in this thesis reveals that Barnes was heading in the right direction by elevating the NATO CCDCOE as a governing body; however, the complex cyber

environment requires a multi-pronged, multilateral approach. His recommendation for the Budapest Convention as a framework should be satisfied in conjunction with the *Tallinn Manual 2.0* restatements and commentary. The best way to achieve effective governance, though, will be to also follow the Paris Climate Agreement model, leverage the Outer Space Treaty, and utilize the international cyber leaders and experts to define a regulatory path. This is only the tip of the iceberg; cyber governance will not be resolved in a short time. However, the intent of this recommended approach is to foster dialogue and creativity in further developing a solution.

#### **4. Legal Venues**

Under the proposed multi-pronged approach, if non-state cyber conflicts cannot be handled multilaterally through the UN Security Council, unilaterally, or through the treaty developed as part of the multi-pronged approach in accordance with the Budapest-Tallinn legal framework, an international court may be an option. Two courts to examine as venues are the ICJ and the International Criminal Court (ICC). As mentioned earlier, the ICJ is available to UN and approved non-UN members for advisory opinions on any legal question—and this could include cyber—especially if the UN includes it in the defined framework. The ICJ thus could be a feasible venue for non-state cyber cases.

The ICC, created under the 1998 Rome Statute, investigates *grave* crimes including crimes against humanity and of aggression.<sup>252</sup> The scope of the ICC’s jurisdiction is narrow and “confined to declarative and symbolic force.”<sup>253</sup> The ICC added the crime of aggression in July 2018. An act of aggression is one that is a “manifest” violation of the UN Charter measured by “its character, gravity, and scale” and that targets state senior officials by a perpetrator who is “in a position effectively to exercises control over or to direct the political or military action of the State which committed the act” and the ICC will only have jurisdiction between ratified state

---

<sup>252</sup> “About,” International Criminal Court, accessed March 10, 2020, <https://www.icc-cpi.int/about>.

<sup>253</sup> Alex Whiting, “Crime of Aggression Activated at the ICC: Does it Matter?” Just Security, December 19, 2017, <https://www.justsecurity.org/49859/crime-aggression-activated-icc-matter/>.

parties.<sup>254</sup> Unless non-state cyber activity is escalated to a *grave* action that can be tied to a physical act of genocide, result in a crime against humanity such as enforced disappearance or torture, or a breach of the Geneva convention as translated to cyber activities (above the threshold of war), the ICC is currently not an appropriate venue for non-state cyber cases.

---

<sup>254</sup> “Elements of Crimes: Crimes of Aggression,” International Criminal Court, Article 8, 43. <https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf>.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. RECOMMENDATIONS AND CONCLUSIONS

The technology age is dynamic, innovative, and expanding each year. International and U.S. cyber strategies, including regulatory measures, need to keep pace if superiority in cyber domain governance is a priority objective. In this new domain, our adversaries assert their influence over U.S. citizens and allies through cyber threats, coercion, privacy invasion, and intimidation without needing to resort to physical aggression. Through this nontraditional method, cyber actors exploit U.S. cyber systems, processes, and vulnerabilities to “gain economic, diplomatic, and military advantages.”<sup>255</sup> Risks of escalated conflict and excessive militarization of the cyber domain could be mitigated through the development and agreement of standing norms, rules of conduct, and regulatory mechanisms for malign cyber activities. Collaboration is a key part of developing international governance, along with effective implementation, proper oversight, and defining roles and processes.

The United States remains the preeminent target for malicious cyber activity, ranging from cyber-enabled economic espionage to cyberattacks targeting government and private-sector business interests. Aligning cyber operations with national policies and international processes is imperative. As part of its role as a global leader, the United States should lead policy development to establish international norms of behavior through established international institutions in the national security environment, to include the UN, the EU, and our Five Eyes (FVEY) partners (“FVEY” refers to an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States). A shift toward a dynamic, comprehensive international governing structure presents numerous potential challenges and responses leveraging a variety of mechanisms that could affect critical infrastructure, business interests, soft targets, and our allies. Determining a calculated response and defining regulation of cyberattacks will enable a whole-of-

---

<sup>255</sup> U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 3.

\* This is not an exhaustive list.

government, whole-of-cyberspace approach that harnesses the United States' role in the global order to respond in a serious and meaningful way.

Intense evaluation and discussion of the United States' role in the cyber domain will enable sustainability in an ever-shifting terrain. Today's adversaries conduct integrated attacks in multiple domains. International regulatory mechanisms can provide positive contributions to U.S. national security, cyber superiority, and adversarial accountability by facilitating cross-domain capabilities across the battlespace environments, which will provide critical commanders and decision makers the strategic information necessary to prevail in the cyber competition.<sup>256</sup>

The United States' deterrence efforts can intensify through persistent engagement and contesting adversaries to show dominance in cyberspace within the boundaries of international law, conduct, and norms.<sup>257</sup> By responding under authorized circumstances, the United States could deter adversaries by a display of strength and intimidation, and contribute to diplomatic relations through faster, adaptable sanctions and communications. U.S. policy, influenced by and interconnected with cyber international laws, will enable the United States and its allies to be powerful, resilient, and push back against cyber threats, proving an equal or stronger playing field that may cause disruptions and a defensive shift for adversary operations.<sup>258</sup>

An international regulatory process will increase response on the U.S. Homefront by eliminating several obstacles associated with the current approvals process, while maintaining civilian oversight. Quicker U.S. responses to malicious threats will provide adversaries with *acknowledgement* of a U.S. presence, knowledge of the threat, and dominance in the domain; it will possibly *disrupt* the malicious threats and *deter* future activity, including lessening the frequency of attacks; and it could have increased *punitive* consequences, such as levying sanctions, issuing indictments, and exposing individual and

---

<sup>256</sup> U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 4.

<sup>257</sup> Joint Chiefs of Staff, *Cyberspace Operations*.

<sup>258</sup> U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority*, 7.

state actors linked to cyberattacks. The faster the United States responds, the sooner it can issue an appropriate remedy.

Cyber success can be based on resiliency, anticipation of vulnerabilities and threats, and defending forward to blunt adversarial action before it severely impacts U.S. networks and infrastructures. A combination of methods may be necessary to enable a stable cyberspace.

Just as the cyber domain is constantly evolving, requiring technical adaptability, so too the international cyber community response needs to remain adaptive in its approach to governance and enforcement. No single platform or solution will address all criminal actors within the cyber domain. This complicated space warrants a multipronged approach for dispute resolution and remedies. The end goal, however, is to obtain the highest-level impact, the biggest-bang-for-buck: ideally, state-imposed remedies and compliance.

Cyberspace is a complex and ambiguous arena that reaches across air, land, sea, and space battlespace domains. As domains grow, cyberattacks will continue to rise and evolve. The existing governance mechanisms may have kept the United States and international partners on pace or just behind its adversaries in the threat landscape. As the volume of data increases, so will vulnerabilities and criminal activity. It is important to push the governance discussion and debate now, rather than wait until adversarial capabilities and homeland vulnerabilities evolve so much that the regulatory discussion becomes more complex and burdensome to the international community. If the United States wants to be a dominant force in the cyber domain, it needs to drive and participate in governance dialogue to include international laws, lexicon, ROE, LOW threshold, conduct, norms, and roles within the cybersphere, as well as propose and assist in the development of mechanisms for regulation of non-state actors. A whole-of-government, whole-of-cyberspace approach should be considered when moving forward.

As discussions continue to revolve around determining the best way to govern the cyber domain, there are several recommended courses of action that need to be developed, researched, and explored further.

## **A. COMPLIANCE AND ENFORCEMENT**

Enforcement will be a challenging issue for cyber governance. Once a framework and governing mechanism is in place, a method for compliance and enforcement should be the final steps in the regulating process. Economic, political, diplomatic, military, and human rights factors should be considered when designing an international compliance and enforcement approach. Several questions should be considered for future exploration:

- What measures should be included for compliance and enforcement of regulatory mechanisms for non-state cyber actors?
- If mandatory cyber sanctions are issued, what would they look like, who or what entity issues them, and how would they be enforced?
- Would multilateral or unilateral sanctions be more effective or would they be dependent on the actor and/or malign cyber activity? Unilateral sanctions, such as economic measures, may be argued to violate international law's Rule Against Intervention—external interference in the internal affairs of a state. But in considering this issue in *Tallinn 2.0*'s Rule 66, the IGE determines that such measures against cyber activities (e.g., prohibiting a state's access to e-commerce websites), does not constitute a violation of the rule. However, the IGE notes that states must be mindful of any treaty and agreement obligations and determine: What would be considered a violation of the rule?
- Sanctions can be controversial, costly, take time to be effective, and often fall short of the ultimate objective: holding a state accountable for activities and practices that are contrary to international law. Are there methods to achieve effective compliance through sanctions or alternative measures? If noncompliance is the result of a resource deficiency, for example, rather than disobedience, what measures could be adopted to provide technical or financial assistance to bring the noncomplying state up to code?

Overall, the compliance and enforcement process and procedures should be determined based on the proposed international regulatory mechanism and framework.

## **B. THE UNITED STATES' ROLE IN INTERNATIONAL GOVERNANCE MECHANISMS**

In consideration of the United States' role in international governing mechanisms, several questions and areas of study should be explored to solidify the U.S. processes and role in support of international governance. The United States should:

- Continue to lead international discussions with governments, international groups of experts, law enforcement, and the private sector for codification of cyber activities to align with international law with the caveat that new cyber-specific laws may need to be created to account for the breadth of cyberspace and the key players within (state, non-state, and proxy state actors). Frameworks and approaches, such as the ones considered in this thesis, should be evaluated and refined or redeveloped to provide a mechanism that is in the best interest of the whole-of-cyberspace. Legal authorities must be adequate to respond to cyber threats.
- Play an integral role in providing clarity to international and domestic law enforcement roles in the cyber governance process.
- Influence the redrawing of international law as it relates to the cyber domain's evolution, thresholds for non-state activities, grounds for attribution, and other cyber concepts that do not fit perfectly into the current international law mold.
- Develop national policies, structures, processes, and best practices across the U.S. federal government to align with international governance mechanisms. Oversight, transparency, and accountability should be addressed to afford our domestic and international partners, as well as civilians, a clear understanding of the United States' regulatory capabilities and limitations.

National security classification guidelines concerning the cyber domain may present a challenge to some of these questions, such as cyber prosecution measures, particularly in regard to information sharing with international partners and publicly available information. As *Tallinn 2.0* points out, most nation-states adopt classified cyber practices, so “publicly available expressions of *opinion juris* are sparse” providing difficulties in the definitive identification of truly cyber-specific customary international law.<sup>259</sup> Cyber threats are long term, requiring the need to protect sensitive sources and methods, especially attribution. Classification should not be a deterrent to coordination and mitigation efforts.

As the literature demonstrates, the United States is facing the beginning stages of a regulated cyber environment. Innovation, techniques, and processes are evolving. Governance approaches need to be further discussed, defined, modified, or abandoned until a workable solution is found. The international community must determine the best approach to implement regulatory measures that will have effective, long-standing value across the cyber domain.

### C. CONCLUSION

Non-state actors pose a challenging problem to cyberspace regulations. Cyber governance cannot be solely based on the concept of sovereignty, promoting state-by-state regulation. Cyber actions cross physical borders, evolve rapidly, and affect the international community’s critical infrastructure, states, cities, and localities. There are very few treaties for cyber activities and those that are in existence are of limited scope and applicability. The *Tallinn 2.0* IGEs are unanimous in their estimations that cyber activities do not exist in a normative void and existing international law applies to cyber operations—a sentiment shared or acknowledged by most nation-states and international organizations, including NATO and the UN Groups of Governmental Experts on Information Security.<sup>260</sup> Formal international governing mechanisms are critical for a unified response and global understanding of the space. Efforts need to involve coordinated partnerships that span

---

<sup>259</sup> Schmitt, *Tallinn Manual 2.0*, 3.

<sup>260</sup> Schmitt, 3.

federal, state, and local levels in the United States, international states, the private sector, and academic subject matter experts to develop and implement effective governance.

The United States is a key player in the cyber domain and needs to fully engage in governance discussions and development to ensure inclusion, intelligence and information sharing, transparency, and accountability. As demonstrated earlier in this thesis, non-state actors pose unique challenges regarding attribution and application of international laws. Focusing on nation-state and proxy-state actors alone will not wholly capture governance of the cyber threat. An international governing mechanism will impact global security and apropos U.S. homeland security by providing clarity on rules and regulation measures for mitigation and response to malign cyber actions by non-state actors.

A secure border is a multilateral, shared effort; difficulties arise when the borders are complex and activity frequently travels across state boundaries. Now is a perfect time to further integrate international representation and cross-border cooperation to increase transparency, joint response, and efficiency in the cyber security effort. Central to partnership cooperation is border management strategies, and international governance mechanisms are the utmost border management strategies concerning cyber activities. During the next several years, it will be difficult to develop an overall solution as there can be “no cookie cutter approaches to developing border security strategies.”<sup>261</sup>

A key lesson learned from this research is that the United States must continue to build and improve cooperation with our national and international partners, as disputes will not be resolved unilaterally. Absolute security against the threats and hazards the country faces is neither fiscally nor operationally possible. Instead, U.S. national security needs to be about managing national risk by “focusing on those actions and interventions that reduce the greatest amount of strategic risk to the Nation.”<sup>262</sup> It must have a holistic, multi-lateral approach that can be found within effective international governance. The issue will not be

---

<sup>261</sup> Rick Nelson et al., “Border Security in a Time of Transformation,” CSIS, July 2010, p. 11.

<sup>262</sup> “Strategic Objective Goal 5.1: Enhance National Preparedness,” Department of Homeland Security, accessed March 26, 2020, <https://obamaadministration.archives.performance.gov/content/goal-51-enhance-national-preparedness-0.html>

solved quickly yet the discussions must continue at full speed to head toward a resolution before the cyber space expands beyond the ability to regulate it.

An effective, multi-pronged international governance approach will be a culmination of enhanced coordinated partnerships and collaborative efforts to provide critical oversight and response to criminal and terrorist activity within the rapidly expanding and evolving cyber problem space. A governance mechanism will provide homeland security benefits for the United States via operational approaches, augmented responses to criminal activity, increased resources for cyber security resilience, and possible deterrence.

.

## LIST OF REFERENCES

- African Union. "African Standby Force (ASF)." Accessed February 29, 2020. <https://www.peaceau.org/en/page/82-african-standby-force-asf-amani-africa-1>.
- . "In a Nutshell." Accessed February 29, 2020. <https://au.int/en/au-nutshell>.
- . "Overview." Accessed February 29, 2020. <https://au.int/en/overview>.
- Alvarez, Edgar. "Sony Pictures Hack: The Whole Story." Engadget. December 10, 2014. <https://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/>.
- Banco, Erin. "FBI Director Christopher Wray Says Russia Remains a Threat to the 2020 Election." Daily Beast. April 26, 2019. <https://www.thedailybeast.com/fbi-director-christopher-wray-says-russia-remains-a-threat-to-2020-election>.
- Barne, Geremie R., and Sang Ye. "The Great Firewall of China." *Wired*. June 1, 1997. <https://www.wired.com/1997/06/china-3>.
- Barnes, Isaac. "Implementation of Active Cyber Defense Measure by Private Entities: The Need for an International Body to Address Disputes." Master's thesis, Monterey, CA: Naval Postgraduate School, 2018. [https://calhoun.nps.edu/bitstream/handle/10945/61274/18Dec\\_Barnes\\_Isaac.pdf?sequence=1&isAllowed=y](https://calhoun.nps.edu/bitstream/handle/10945/61274/18Dec_Barnes_Isaac.pdf?sequence=1&isAllowed=y).
- BBC. "Cyber-attack: U.S. and UK blame North Korea for WannaCry." December 19, 2017, <https://www.bbc.com/news/world-us-canada-42407488>.
- Brandes, Sean, "The Newest Warfighting Domain: Cyberspace." *Synesis Journal of Science, Technology, Ethics, and Policy* (2013), [http://www.synesisjournal.com/vol4\\_g/Brandes\\_2013\\_G90-95.pdf](http://www.synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf).
- Brumfield, Cynthia. "New CISA Director Outlines Top 5 Priorities for Protecting U.S. Critical Infrastructure." CSO. March 6, 2019. <https://www.csoonline.com/article/3353638/new-cisa-director-outlines-top-5-priorities-for-protecting-u-s-critical-infrastructure.html>.
- Burr, Richard. "Senate Select Committee on Intelligence." [burr.senate.gov](http://burr.senate.gov). July 3, 2018, <https://www.burr.senate.gov/download/final-ssci-ica-assessment>.
- Casey, Lee, and David B. Rivkin. "International Law and the Nation-State at the U.N.: A Guide for U.S. Policymakers." Heritage Foundation. August 18, 2016. <https://www.heritage.org/global-politics/report/international-law-and-the-nation-state-the-un-guide-for-us-policymakers>.
- CCDCOE. "About Us." CCDCOE. <https://ccdcoe.org/about-us/>.

- Central Intelligence Agency. "Executive Order 12333." <https://www.cia.gov/about-cia/eo12333.html>. Accessed November 21, 2018.
- Chakhak, Elias. "Winter Olympics Cyber Attack Signs Point to Russia—So Why the False-Flag?" Cyber Research Databank. Accessed March 22, 2020. <https://www.cyberdb.co/winter-olympics-cyber-attack-all-signs-point-to-russia/>.
- Chernenko, Elena, Oleg Demidov, and Fyodor Lukyanov. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council on Foreign Relations, February 23, 2018. <https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms>
- Coats, Daniel R. "Worldwide Threat Assessment of the U.S. Intelligence Community." Office of the Director of National Intelligence, January 29, 2019. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.
- Condon, Stephanie, "DHS Chief: U.S. to Take More Aggressive Posture against Cyber Attackers." April 17, 2018. <https://www.zdnet.com/article/dhs-chief-us-to-take-more-aggressive-posture-against-cyber-attackers/>.
- Constine, Josh. "ISIS CyberCaliphate Hacks U.S. Military Command Accounts." TechCrunch, January 12, 2015. <https://techcrunch.com/2015/01/12/cyber-caliphate/>.
- Cooper, Helene. "ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts." *New York Times*, January 12, 2015. <https://www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html>.
- Council of Europe. *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*. ETS No. 89, January 3, 2006. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>.
- . "Details of Treaty No. 185, Convention on Cybercrime." November 23, 2001. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.
- . "T-CY Work Plan for the Period 1 January 2018—31 December 2019." November 27, 2018. <https://rm.coe.int/t-cy-2018-27-tcy-workplan-v6adopted/16808feb6c>.
- Council on Foreign Relations. "Indictment of PLA Officers." May 2014. <https://www.cfr.org/interactive/cyber-operations/indictment-pla-officers>.
- Council on Foreign Relations (blog). "What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?" September 10, 2018. <https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations>.

- Crowdstrike, “2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed.” Accessed January 3, 2020. [https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gr?utm\\_campaign=Threat\\_Report\\_2019&utm\\_medium=Web&utm\\_source=Marketo](https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gr?utm_campaign=Threat_Report_2019&utm_medium=Web&utm_source=Marketo).
- Cyber Tech Accord. “Objective.” Accessed October 31, 2018. <https://cybertechaccord.org/about/>.
- Cybersecurity and Infrastructure Security Agency. “CISA Regional Service Delivery Model Fact Sheet.” Accessed February 24, 2020. <https://www.cisa.gov/publication/cisa-regional-service-delivery-model-fact-sheet>.
- . “Hidden Cobra—North Korean Malicious Cyber Activity.” Accessed 8/3/2019. <https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity>.
- d’Aspremont, Jean, André Nollkaemper, Ilias Plakokefalos, and Cedric Ryngaert. “Sharing Responsibility Between Non-State Actors and States in International Law: Introduction.” *Netherlands International Law Review* 62, 49–67 (2015). <https://doi.org/10.1007/s40802-015-0015-0>.
- DarkOwl. “Nation-State Actors on the DarkNet.” (blog). January 2, 2020. <https://www.darkowl.com/blog-content/nation-state-actors-on-the-darknet>.
- DeGuerin, Mack/ “U.S. Silently Enters New Age of Cyberwarfare.” *New York Magazine*, September 2018. <http://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html>.
- Department of Defense. *Cyber Strategy 2018*. Washington, DC: Department of Defense, 2018. [https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).
- . *The DOD Cyber Strategy*. Washington, DC: Department of Defense, 2015. [http://archive.defense.gov/home/features/2015/0415\\_cyber-strategy/final\\_2015\\_DOD\\_cyber\\_strategy\\_for\\_web.pdf](http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_DOD_cyber_strategy_for_web.pdf).
- . *DOD Digital Modernization Strategy 2019*. Washington, DC: Department of Defense, 2019. <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>.
- . *Law of War Manual*. Washington, DC: Department of Defense, 2016. <https://dod.defense.gov/Portals/1/Documents/pubs/DOD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>.

- Department of Homeland Security. “National Protection and Programs Directorate (NPPD) at a Glance.” Accessed November 15, 2018. <https://www.dhs.gov/publication/nppd-glance>.
- . “Organizational Chart.” Accessed March 1, 2020. <https://www.dhs.gov/organizational-chart>.
- . “Preventing and Defending Against Cyber Attacks,” 2011. <https://www.dhs.gov/news/2011/10/18/preventing-and-defending-against-cyber-attacks>.
- . “Strategic Objective Goal 5.1: Enhance National Preparedness.” Accessed March 26, 2020. <https://obamaadministration.archives.performance.gov/content/goal-51-enhance-national-preparedness-0.html>
- Department of Justice. “Avalanche Network Dismantled in International Cyber Operation.” Press Release No.: 16–1422, December 5, 2016.
- Department of State. “Bureau of Diplomatic Security.” Accessed November 14, 2018. <https://www.state.gov/m/ds/>.
- . “Diplomacy 101.” Accessed October 5, 2018. <https://www.state.gov/discoverdiplomacy/diplomacy101/issues/170614.htm>.
- . “International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms.” Accessed March 22, 2020. <https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm>.
- . *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*. Article VI, (Washington, 1967). <https://2009-2017.state.gov/t/isn/5181.htm>.
- Department of State, Office of the Historian. “National Security Act of 1947.” Accessed November 20, 2018. <https://history.state.gov/milestones/1945-1952/national-security-act>.
- EPIC. “EPIC v. NSA: NSPD-54 Appeal Freedom of Information Act.” Accessed November 18, 2018. <https://epic.org/foia/nsa/nspd-54/appeal/>.
- European Union. “The EU in Brief.” Accessed February 29, 2020. [https://europa.eu/european-union/about-eu/eu-in-brief\\_en](https://europa.eu/european-union/about-eu/eu-in-brief_en).
- Federal Bureau of Investigation. “Terrorism: Terrorism Definitions.” Accessed January 13, 2020. <https://www.fbi.gov/investigate/terrorism>.

- Fidler, David. "The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers." Council on Foreign Relations, March 15, 2018. <https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers>.
- Freedberg, Jr., Sydney. "Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff." *Breaking Defense*, September 17, 2018. <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.
- Fruhlinger, Josh. "Top Cybersecurity Figures, Facts, and Statistics for 2018." CSO. October 10, 2018. <https://www.csoononline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html>.
- . "What Is WannaCry Ransomware, How Does It Infect, And Who Was responsible?" CSO. Accessed November 11, 2018. <https://www.csoononline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>.
- GCHQ. "Welcome to GCHQ." Accessed October 28, 2018. <https://www.gchq.gov.uk/>.
- Global Security. "Gulf Cooperation Military Guide." Accessed February 29, 2020. <https://www.globalsecurity.org/military/world/gulf/index.html>.
- Graff, Garret. "How the U.S. Forced China to Quit Stealing—Using a Chinese Spy." *Wired*, October 11, 2018. <https://wired.com/story/us-china-cybertheft-su-bin>.
- Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*. Accessed November 3, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- Group of Governmental Experts. Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly, Sixty-Eighth Session, (2013). <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf>.
- Gulf Cooperation Council. "About GCC." Accessed February 29, 2020. <https://www.gcc-sg.org/en-us/AboutGCC/Pages/StartingPointsAndGoals.aspx>.
- Hern, Alex. "Cyber-Attacks and Hacking: What You Need To Know." *Guardian*. November 1, 2016. <https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime>.
- . "WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017." *Guardian*, December 30, 2017. <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware>.

- Howell O'Neill, Patrick. "DNI: Chinese Hacking Against U.S. Companies Is 'Ongoing' But 'Significantly Reduced.'" Cyberscoop, May 23, 2017. <https://www.cyberscoop.com/china-us-hacking-odni-dan-coats-2017/>.
- Infosec Institute. "The Time Has Come for Rules of Engagement for Cyberwarfare." Accessed November 15, 2018. <https://resources.infosecinstitute.com/the-time-has-come-for-rules-of-engagement-for-cyberwarfare/#gref>.
- International Criminal Court. "About." Accessed March 10, 2020. <https://www.icc-cpi.int/about>.
- . "Elements of Crimes: Crimes of Aggression." Article 8 bis, 43. <https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf>.
- INTERPOL. "Cybercrime." Accessed February 29, 2020. <https://www.interpol.int/en/Crimes/Cybercrime>.
- . "What Is INTERPOL?" Accessed February 29, 2020. <https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>.
- . "The Constitution of the ICPO-INTERPOL. Articles 2, 3, 9 (Vienna–1956), Amended 2017." <https://www.interpol.int/content/download/590/file/Constitution%20of%20the%20ICPO-INTERPOL-EN.pdf>
- Jensen, Eric T. "The Tallinn Manual 2.0: Highlights and Insights." 2017. *Georgetown Journal of International Law* 735, no. 48 (March 2017) 735–778.
- Joint Chiefs of Staff. *Cross-Domain Synergy in Joint Operations: Planner's Guide*. Washington, DC: Joint Chiefs of Staff, 2016. [http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross\\_domain\\_planning\\_guide.pdf?ver=2017-12-28-161956-230](http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230).
- . *Cyberspace Operations*. JP 3-12. Washington, DC: Joint Chiefs of Staff, 2018. [https://fas.org/irp/DODdir/DOD/jp3\\_12.pdf](https://fas.org/irp/DODdir/DOD/jp3_12.pdf).
- . *Doctrine for Joint Operations*. JP 3-0. Washington, DC: Joint Chiefs of Staff, 1995. <http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>.
- . *Implementation of the DOD Law of War Program*. CJCSI 5810.01D. Washington, DC: Joint Chiefs of Staff, 2010. <http://www.jcs.mil/LinkClick.aspx?fileticket=xsR7uIFHy4o%3D&tabid=19767&portalid=36&mid=46626>.
- . *Legal Support to Military Operations*. JP 1-04. Washington, DC: Joint Chiefs of Staff, 2016. [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1\\_04.pdf](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_04.pdf).

- Koh, David. "Atlantic Council Eighth Annual International Conference on Cyber Engagement (ICCE): Introductory Remarks." Symposium, G.W. Lisner Auditorium, George Washington University, Washington, DC, April 22, 2019. <https://www.atlanticcouncil.org/icce>.
- Koh, Harold Hongju. "International Law in Cyberspace." USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012. <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>.
- Lapowsky, Issie. "How Russian Facebook Ads Divided and Targeted U.S. Voters Before the 2016 Election." *Wired*. April 16, 2018. <https://www.wired.com/story/russian-facebook-ads-targeted-us-voters-before-2016-election/>.
- Lotrionte, Catherine. "Atlantic Council Eighth Annual International Conference on Cyber Engagement (ICCE): Introductory Remarks." Symposium, G.W. Lisner Auditorium, George Washington University, Washington, DC, April 22, 2019. <https://www.atlanticcouncil.org/icce>.
- Lyu, Jinghua. "What Are China's Cyber Capabilities and Intentions?" IPI Global Observatory. April 1, 2019. <https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734>.
- Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press: 2018.
- McLeary, Paul. "Pentagon: Hacking of CENTCOM Site a Prank." *Defense News*, January 12, 2015. <https://www.defensenews.com/opinion/intercepts/2015/01/12/pentagon-hacking-of-centcom-site-a-prank/>.
- Mehta, Aaron. "Mattis Reveals New Rules of Engagement." *Military Times*, October 3, 2017. <https://www.militarytimes.com/flashpoints/2017/10/03/mattis-reveals-new-rules-of-engagement/>.
- Miller, Greg, Ellen Nakashima, and Adam Entous. "Obama's Secret Struggle to Punish Russia for Putin's Election Assault." *Washington Post*, June 23, 2017, [https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm\\_term=.3ecae726ee00](https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.3ecae726ee00).
- Morgan, Steve. "Global Ransomware Damage Costs Predicted To Exceed \$5 Billion In 2017," *Cybercrime Magazine*, May 18, 2017. <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/>.
- Nakashima, Ellen. "White House Says Sony Hack Is A Serious National Security Matter." *Washington Post*, December 18, 2014. [https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25\\_story.html?noredirect=on&utm\\_term=.263af0131909](https://www.washingtonpost.com/world/national-security/white-house-says-sony-hack-is-a-serious-national-security-matter/2014/12/18/01eb8324-86ea-11e4-b9b7-b8632ae73d25_story.html?noredirect=on&utm_term=.263af0131909).

- Nash, Kim S. "One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs." *Wall Street Journal*, June 27, 2018. <https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906>.
- National Cyber Security Centre. "Turla Revealed As Exploiting Iranian Hacking Tools And Techniques To Attack Dozens Of Countries." October 21, 2019. <https://www.ncsc.gov.uk/news/turla-group-behind-cyber-attack>.
- National Intelligence Council. "Nonstate Actors: Impact on International Relations and Implications for the United States." 2007. [https://www.dni.gov/files/documents/nonstate\\_actors\\_2007.pdf](https://www.dni.gov/files/documents/nonstate_actors_2007.pdf).
- NATO Communications and Information Agency. "Cyber Security." Accessed January 12, 2020, <https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx>.
- . "NATO Industry Cyber Partnership (NICP)." Accessed January 12, 2020, <https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx>.
- NATO. "NATO Cyber Defence," Fact Sheet, July 2016, [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2016\\_07/20160627\\_1607-factsheet-cyber-defence-eng.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf).
- . "NATO, European Union Experts Review Cyber Defence Cooperation." December 17, 2019, [https://www.nato.int/cps/en/natohq/news\\_172157.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/news_172157.htm?selectedLocale=en).
- . "Collective Defence." Accessed February 24, 2020. [https://www.nato.int/cps/en/natohq/topics\\_110496.htm](https://www.nato.int/cps/en/natohq/topics_110496.htm).
- . "Cyber Defence," September 6, 2019, [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm).
- . "London Declaration: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council." Press Release 115. December 4, 2019. [https://www.nato.int/cps/en/natohq/official\\_texts\\_171584.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_171584.htm?selectedLocale=en).
- . "Member Countries." Accessed January 15, 2020, [https://www.nato.int/cps/en/natolive/topics\\_52044.htm](https://www.nato.int/cps/en/natolive/topics_52044.htm).
- . "NATO Defence Planning Process." Accessed March 22, 2020, [https://www.nato.int/cps/en/natohq/topics\\_49202.htm](https://www.nato.int/cps/en/natohq/topics_49202.htm).
- . "NATO Enlargement." Accessed January 15, 2020, <https://www.nato.int/nato-welcome/index.html>.

- . “NATO International Staff.” Accessed January 15, 2020, [https://www.nato.int/cps/en/natohq/who\\_is\\_who.htm](https://www.nato.int/cps/en/natohq/who_is_who.htm).
- NTT Group. “NTT Joined Cybersecurity Tech Accord, A Growing Global Industry Agreement To Protect Users And Customers Everywhere.” October 31, 2018. [https://www.ntt.co.jp/topics\\_e/techaccord/index.html](https://www.ntt.co.jp/topics_e/techaccord/index.html).
- Nye, Jr., Joseph S. “Unilateralism vs. Multilateralism.” *International Herald Tribune*, June 13, 2012. <https://www.globalpolicy.org/component/content/article/199/41054.html>.
- O’Brien, William V. *The Conduct of Just and Limited War*. Westport, CT: Praeger Publishing, 1981).
- Obama, Barack. *Securing U.S. Cyber Infrastructure*. Washington, DC: American Rhetoric Online Speech Bank, 2009.
- Office of Personnel Management. “Cybersecurity Resource Center, What Happened.” Accessed July 28, 2019. <https://www.opm.gov/cybersecurity/cybersecurity-incidents/>.
- Office of the Director of National Intelligence. “A Guide to Cyber Attribution.” September 14, 2018. [https://www.dni.gov/files/CTIIC/documents/ODNI\\_A\\_Guide\\_to\\_Cyber\\_Attribution.pdf](https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf).
- Olenic, Doug. “Turla Cyberespionage Group Switched to Open-Source Malware.” *SC Magazine*. May 22, 2018. <https://www.scmagazine.com/home/security-news/malware/turla-cyberespionage-group-switched-to-open-source-malware/>.
- Palmer, Danny. “Russian Hackers Are Attacking Home Routers, ISPs And Business Firewalls To Spy And Steal Data, Warns U.S., UK.” *ZD Net*. April 16, 2018. <https://www.zdnet.com/article/russian-hackers-are-attacking-home-routers-isps-and-business-firewalls-to-spy-and-steal-data-warns/>.
- Parsons, Ed, and Michael Raff. “Understanding the Cyber Threat from Russia.” *F-Secure*. Accessed March 22, 2020. <https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-russia>.
- Raymond, Adam. “Trump Makes It Easier for the Military to Launch Cyberattacks.” *New York Magazine*. August 16, 2018. <http://nymag.com/intelligencer/2018/08/trump-makes-it-easier-for-the-u-s-to-launch-cyber-attacks.html?gtm=top&gtm=bottom>.
- Rivera, Jason. “Understanding and Countering Nation-State Use of Protracted Unconventional Warfare,” *Small Wars Journal* (Online), accessed February 22, 2020. <https://smallwarsjournal.com/jrnl/art/understanding-and-countering-nation-state-use-of-protracted-unconventional-warfare>.

- Robinson, Teri. "FBI Director Wray Says Cyber-threats 'Bigger Than Government.'" *SC Magazine*. March 7, 2019. <https://www.scmagazineuk.com/fbi-director-wray-says-cyber-threats-bigger-government/article/.1578178>.
- Rollins, John W. "U.S.-China Cyber Agreement." *Congressional Research Service*. October 16, 2015. <http://www.fas.org/sgp/crs/index.html>.
- Rosenzweig, Paul. "Operation Olympic Games Legal Setback and Strategic Opportunity." *Lawfare*. September 16, 2012. <https://www.lawfareblog.com/operation-olympic-games-legal-setback-and-strategic-opportunity-guest-post-ernesto-j-sanchez>.
- Sanger, David, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict." *New York Times*, June 17, 2018. <https://www.nytimes.com/2018/06/17/us/politics/cyber-command-trump.html>.
- . "Tech Firms Sign 'Digital Geneva Accord' Not to Aid Governments in Cyberwar." *New York Times*, April 17, 2018., <https://www.nytimes.com/2018/04/17/us/politics/tech-companies-cybersecurity-accord.html>.
- Schmaglowski, Dieter. "The NATO Defence Planning Process (NDPP): An Overview," NATO Standardization Office. October 30, 2018. [https://www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/2018%20International%20Standardization%20Workshop/20181030--Item3-NDPPOverview-IntlStdznWorkshop\\_Schmaglowski.pdf?ver=2018-11-06-151624-033](https://www.dsp.dla.mil/Portals/26/Documents/Publications/Conferences/2018/2018%20International%20Standardization%20Workshop/20181030--Item3-NDPPOverview-IntlStdznWorkshop_Schmaglowski.pdf?ver=2018-11-06-151624-033).
- Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. New York: Cambridge University Press. 2017.
- Schmitt, Michael, and Sean Fahey. "WannaCry and the International Law of Cyberspace." *Just Security*. December 22, 2017. <https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/>.
- Seals, Tara. "One Year After WannaCry: A Fundamentally Changed Threat Landscape." *Threat Post*. May 17, 2018. <https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/>.
- Segal, Adam. "An Update on U.S.-China Cybersecurity Relations." *Council on Foreign Relations* (blog). November 17, 2017. <https://www.cfr.org/blog/update-us-china-cybersecurity-relations>.
- . "When China Rules the Web: Technology in Service of the State." *Foreign Affairs*, September 2018. <https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web>.

- Seger, Alexander. "The Budapest Convention on Cybercrime: A Framework for Capacity Building." *Global Cyber Expertise Magazine*, 2 (2016).
- Seppala, Timothy. "Sony Pictures Hack Takes Computers Down Studio-Wide." Engadget. November 24, 2014. <https://www.engadget.com/2014/11/24/sony-pictures-hack/>.
- Sigholm, Johan. "Non-State Actors in Cyberspace Operations." *Journal of Military Studies*, 4, no. 11. November 23, 2016. <https://doi.org/10.1515/jms-2016-0184>.
- Theohary, Catherine A., and Cory Welt. "Russia and the U.S. Presidential Election." Congressional Research Service, January 17, 2017. <https://fas.org/sgp/crs/natsec/IN10635.pdf>.
- UNFCCC. "Ad Hoc Working Group of the Paris Agreement (APA)." Accessed February 28, 2020. <https://unfccc.int/process/bodies/subsidiary-bodies/apa>.
- . "Nationally Determined Contributions (NDCs)." Accessed February 28, 2020. <https://unfccc.int/process-and-meetings/the-paris-agreement/nationally-determined-contributions-ndcs>.
- . "The Paris Agreement." Accessed February 28, 2020. <https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement>.
- . "Transparency and Reporting." Accessed February 28, 2020. <https://unfccc.int/process-and-meetings/transparency-and-reporting/the-big-picture/what-is-transparency-and-reporting>.
- United Nations. "2020 United Nations Framework on Climate Change, Paris Agreement- Status of Ratification." Accessed February 28, 2020. <https://unfccc.int/process/the-paris-agreement/status-of-ratification>.
- . "Chapter I: Purposes And Principles." Article 2(1). <https://www.un.org/en/sections/un-charter/chapter-i/index.html>.
- . "Chapter II: Membership." Article 2(3). <https://www.un.org/en/sections/un-charter/chapter-i/index.html>.
- . "Chapter VI: Pacific Settlement Of Disputes." Article 33(1). <https://www.un.org/en/sections/un-charter/chapter-vi/index.html>.
- . "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression." Accessed March 22, 2020. <https://www.un.org/en/sections/un-charter/chapter-vii/index.html>.
- . "Chapter XIV: The International Court of Justice." Article 93. <https://www.un.org/en/sections/un-charter/chapter-xiv/index.html>.

- . “Chapter XVII: Transitional Security Arrangements.” Article 106.  
<https://www.un.org/en/sections/un-charter/chapter-xvii-0/index.html>.
- . “Chapter XXVII, Charter of the United Nations and Statute of the International Court of Justice: Paris Agreement.” December 12, 2015. [https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=XXVII-7-d&chapter=27&clang=\\_en](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVII-7-d&chapter=27&clang=_en).
- . “United Nations and the Rule of Law.” Accessed October 4, 2018,  
<https://www.un.org/ruleoflaw/what-is-the-rule-of-law/>.
- . “United Nations Urged to Pay More Heed to Role of ‘Non-State Actors’ in Approach to Global Problems.” June 21, 2004. <https://www.un.org/press/en/2004/sg2089.doc.htm>.
- United Nations Office for Disarmament Affairs. “Developments in the Field of Information and Telecommunications in the Context of International Security.” 2011. <https://www.un.org/disarmament/ict-security/>.
- U.S. Cyber Command, *2018 Cyberspace Strategy Symposium Proceedings*. Fort Meade, MD: U.S. Cyber Command, 2018. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427>.
- U.S. Cyber Command. “About History.” Accessed October 1, 2018.  
<https://www.cybercom.mil/About/History>.
- . “About Mission and Vision.” Accessed October 1, 2018.  
<https://www.cybercom.mil/About/Mission-and-Vision/>.
- . *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*. Fort Meade, MD: U.S. Cyber Command, 2018.  
<https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.
- U.S. Government Accountability Office. *Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*. GAO-19-128. Washington, DC: Government Accountability Office, 2018. <https://www.gao.gov/assets/700/694913.pdf>.
- U.S. Marine Corps Basic School. *Law of War/Introduction to Rules of Engagement B130936 Student Handout*. Camp Barrett, VA: United States Marine Corps.  
<https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B130936%20Law%20of%20War%20and%20Rules%20Of%20Engagement.pdf>.

- U.S. Senate. "Senate Select Committee on Intelligence," July 3, 2018, <https://www.intelligence.senate.gov/publications/committee-findings-2017-intelligence-community-assessment>.
- Vicens, A. J. "The U.S. Government Has Done 'Almost Nothing' to Stop Cyber Attacks," *MotherJones*, July 16, 2019, <https://www.motherjones.com/politics/2019/07/the-us-government-has-done-almost-nothing-to-stop-cyber-attacks/>.
- Volz, Dustin. "Trump Signs Into Law U.S. Government Ban on Kaspersky Lab Software." Reuters, December 12, 2017. <https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4>.
- Walters, Riley. "Federal Cyber Breaches in 2017," *The Heritage Foundation*, January 3, 2018, <https://www.heritage.org/cybersecurity/report/federal-cyber-breaches-2017>.
- Weber, Valentin. "Linking Cyber Strategy with Grand Strategy: The Case of the United States." *Journal of Cyber Policy* 3, no. 2 (August 17, 2018): 236–257. <https://doi.org/10.1080/23738871.2018.1511741>.
- White House, The. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: White House, 2011. [https://obamawhitehouse.archives.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).
- . *National Strategy for Counterterrorism*. Washington, DC: White House, 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf>.
- . *National Cyber Strategy of the United States of America*. Washington, DC: 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
- . *National Security Strategy of the United States of America*. December 18, 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- Whiting, Alex. "Crime of Aggression Activated at the ICC: Does it Matter?" Just Security, December 19, 2017. <https://www.justsecurity.org/49859/crime-aggression-activated-icc-matter/>.
- Whittaker, Zach. "FBI Says North Korea Is 'Responsible' For Sony Hack, As White House Mulls Response." ZDNet. December 19, 2014. <https://www.zdnet.com/article/us-government-officially-blames-north-korea-for-sony-hack/>.
- Williams, Oscar. "Microsoft Reveals Scale of Nation-State Attacks Targeting Customers." New Statesman, July 18, 2019. <https://tech.newstatesman.com/security/microsoft-customers-nation-state-hackers>.

Wong, Joan. "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History." *Wired*. October 17, 2019. <https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/>.

Woo, Kim Chong. "The Evolution of North Korean Cyber Threats." Asan Institute, February 20, 2019, <http://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/>.

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California