Standardizing States' Response to Cyberattacks: The United Nations' Opportunity to Normalize Behavior

A Monograph

by

Lt Col Kyle A. Benwitz
US Air Force

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2018

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
19-06-2017	Master's Thesis	June 2017 – May

4. TITLE AND SUBTITLE
Standardizing States' Response to Cyberattacks: The United Nations' Opportunity to Normalize Behavior

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lt Col Kyle A. Benwitz

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies (SAMS)
201 Reynolds Avenue
Fort Leavenworth, KS 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
731 McClellan Avenue
Fort Leavenworth, KS 66027-1350

10. SPONSOR/MONITOR'S ACRONYM(S)
CGSC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The nature and risks of cyberspace create effects that influence a state's national security and interests. These effects, individual non-state actors directly engaging states, a lower threshold for offensively responding to cyberattacks, and the pace of cyberspace's modernization, deepen tension between states and increase the likelihood of state-initiated armed conflict in response to cyberattacks. Additionally, it is important that states appreciate the efficacy of internationally agreed-upon behavioral standards in cyberspace and how they improve global stability and increase security. To alleviate the possibility of a state responding disproportionately to a cyberattack from an actor in cyberspace, states must implement international standards of behavior that provide a baseline for responses to cyberattacks that are acceptable to the international community. It is possible for a multilateral, global alliance to successfully develop and implement these behavioral norms. Further, the United Nations is the preferred venue to develop and approve a set of internationally agree-upon standards.

15. SUBJECT TERMS
US Cybersecurity, Cyberspace, Cyberattack, Cyberspace Standards and Norms, Alliances

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Lt Col Kyle A. Benwitz
Unclassified	Unclassified	Unclassified		51	19b. TELEPHONE NUMBER *(include area code)* 856-381-2065

Monograph Approval Page

Name of Candidate: Lieutenant Colonel Kyle A. Benwitz

Monograph Title: Standardizing States' Response to Cyberattacks: The United Nations' Opportunity to Normalize Behavior

Approved by:

_____, Monograph Director
Melissa A. Thomas, PhD

_____, ASLSP Director
Barry M. Stentiford, PhD

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 24th day of May 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

Standardizing States' Response to Cyberattacks: The United Nations' Opportunity to Normalize Behavior, by Lt Col Kyle A. Benwitz, USAF, 51 pages.

The nature and risks of cyberspace create effects that influence a state's national security and interests. These effects, individual non-state actors directly engaging states, a lower threshold for offensively responding to cyberattacks, and the pace of cyberspace's modernization, deepen tension between states and increase the likelihood of state-initiated armed conflict in response to cyberattacks. Additionally, it is important that states appreciate the efficacy of internationally agreed-upon behavioral standards in cyberspace and how they improve global stability and increase security.

To alleviate the possibility of a state responding disproportionately to a cyberattack from an actor in cyberspace, states must implement international standards of behavior that provide a baseline for responses to cyberattacks that are acceptable to the international community. It is possible for a multilateral, global alliance to successfully develop and implement these behavioral norms. Further, the United Nations is the preferred venue to develop and approve a set of internationally agreed-upon standards.

Contents

Acknowledgement

I want to express my sincerest appreciation to Dr. Melissa Thomas, Associate Professor of Social Science, School of Advanced Military Studies, Fort Leavenworth, Kansas, for her inexhaustible patience and articulate editing skills over the many months of research and writing. Additionally, I offer my thanks to Colonel Yannick Michaud and the members of the Advanced Strategic Leadership Studies Program, School of Advanced Military Studies, Fort Leavenworth, Kansas, for their enduring support and humor throughout this process. Most importantly, I want to thank my wife, Michelle, and children, Zoe and Jackson, for their unwavering encouragement and positive attitude during the many hours spent completing this project.

Acronyms

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASEAN	Association of Southeast Asian Nations
DDoS	Distributed Denial of Service
EU	European Union
GGE	Group of Governmental Experts
ITU	International Telecommunications Union
ITU-T	ITU Telecommunications Standardization Sector
NATO	North Atlantic Treaty Organization

Figures

Introduction: Escalation Without End

> My life, like that of most people on the planet, was transformed by the Second World War…I drew from the failure of appeasement the lesson that aggression must always be firmly resisted. But how? The ultimate victory of the Allies persuaded me that nations must co-operate in the defence of agreed international rules if they are either to resist great evils or to achieve great benefits. That is merely a platitude, however, if political leaders lack the courage and farsightedness, or – what is equally important – if nations lack strong bonds of common loyalty. Weak nations could not have resisted Hitler effectively – indeed, those nations that were weak did not stand up to him. So I drew from the Second World War a lesson very different from the hostility toward the nation-state evinced by some post-war European statesmen. My view was – and is – that an effective internationalism can only be built by strong nations which are able to call upon the loyalty of citizens to defend and enforce civilized rules of international conduct.
>
> —Margaret Thatcher, *The Downing Street Years*

In the late 1960s, the Advanced Research Projects Agency (ARPA) developed a rudimentary "internet" called ARPA Network (ARPANET) to communicate and share data collaboratively between its headquarters and satellite research facilities. Within months, analysts had postulated means to infiltrate networks like ARPANET and established the concept for what would become known as computer and internet hacking.[1]

Over time, risks to state's economy and national security as a result of state and non-state-sponsored operations in cyberspace have grown exponentially with parallel advancements in technology. States reported economic losses attributed to cybercrime in 2012 ranging from 3.1 million to 8.5 million dollars for Great Britain, Australia, the United States, and Germany with a predicted increase in costs of 40 percent annually based on an average of 1.8 successful cyberattacks per week.[2] The weaponization of cyberspace poses a significant risk to a state's national security as evidenced by the remote destruction of a Soviet pipeline system via

---

[1] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York, NY: Simon & Schuster, 2016), 7-9.

[2] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," *Transatlantic Academy Paper Series*, no. 1 (2014): 6, accessed September 26, 2017, http://www.transatlanticacademy.org/site/default/files/publications/Bendiek_TestsofPartnership_Feb14_web.pdf. The author converted the article's listed values of 2.5 million and 6.9 million Euros to dollars.

cyberattack in 1982, the Russian Federation's use of offensive cyberspace operations preceding land force operations across the border into Georgia in 2008, and the destruction of Iranian centrifuges via cyberattack in 2010.[3]

States' responses to provocations from actors in cyberspace are inconsistent due in part to the difficulty of attributing an act to an actor, to a wide variance in countries' capability to respond, and to a lack of an international agreement on acceptable responses. Governments continue work aimed at defining when it is appropriate to respond to a cyberattack, yet there is little effort focused on defining an acceptable response when an attack meets a predetermined threshold. For instance, the United States Senate Committee on Foreign Relations submitted, for the first time, a bill in May 2016 that sought to define cyber actions that constituted an act of war, which in turn would allow the use of international law to respond to cyberattacks.[4] By not tempering the response options to cyberattacks, the bill does not constrain political leaders from considering all response options to acts of war. This could increase the possibility of an overreaction to a cyberattack since there are no limits on how the state should respond. Because governments employ a variety of means to combat and defend against these dangers, there is a possibility for unintended conflict escalation as nations attempt to outdo each other in order to gain or maintain an advantage in the cyber domain.

The international community must understand the relationship between the risks and effects associated with the nature of cyberspace and their influence on a state's national security

---

[3] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, The Royal Institute of International Affairs Report (London: Chatham House, 2010), 7, accessed September 26, 2017, https://pdfs.semanticscholar.org/194c/24d15590a0cc6b39658db996eba85600cff8.pdf; Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," *Defence Studies* 15, no. 4 (December 2015): 301, accessed September 26, 2017, https://doi.org/10.1080/14702436.2015.1108108.

[4] Joshua A. Mendoza, "Cyber Attacks and the Legal Justification for Armed Response," Monograph (US Army Command and General Staff College, 2017), 10.

and interests. Additionally, it is important that states appreciate the efficacy of internationally agreed-upon behavioral standards and how they improve global stability and increase security.

To alleviate the possibility of a state responding disproportionately to a cyberattack from an actor in cyberspace, states must implement international standards of behavior that provide a baseline for acceptable responses to cyberattacks. It is possible for a multilateral, global alliance to successfully develop and implement these behavioral norms. Further, the United Nations is the preferred venue to develop and approve a set of internationally agreed-upon standards.

In Section 1, the monograph will explore the nature of cyberspace and its associated risks to and effects on a state's national security and interests. This discussion provides support for a recommendation to implement international standards of behavior for responding to cyberattacks. Section 2 will discuss three types of alliances, international alliances' efforts to develop viable behavioral norms in cyberspace, and the limitations of alliances that reduce the possibility of successfully developing and adopting international standards. Finally, Section 3 will begin by presenting arguments against the idea that alliances are the best means to draft and implement agreed-upon norms then offer evidence to refute the arguments. The section will end with on-going successes of the United Nations that provide a proof of principle for successfully developing and adopting international standards of behavior for responding to cyberattacks.

This monograph will not address the legality of responding to provocations from actors in cyberspace nor acceptable options for countries to consider when responding to actions from the cyber domain. Rather, its focus is to present an argument supporting the efforts of states to engage each other via the United Nations in order to develop and adopt behavioral norms for responding to cyberattacks.

The Cyberspace Environment Could Use Some Standards

The global and borderless nature of cyberspace presents risks to states' ability to control and govern their own interests and infrastructure. One of the primary risks to a state's cybersecurity and defense is the potential for the government to overreact to an actor's

provocations in the cyber domain which could lead to an armed conflict. This risk is not only in response to the original cyberattack, but also to the threat of a state losing its perceived asymmetric advantage in cyberspace over its adversary. Countries around the world view their environment through the lenses of differing values and interests which lead to a wide array of threat and risk assessments. In an effort to moderate a government's reaction to an actor's activities in cyberspace, states must develop and use a common lens or standard of behavior that provides a framework for determining the proper response to aggressive actions. This section will review the characteristics of cyberspace and the risks and effects associated with its nature that have the potential to lead states to favor employing a disproportionate amount of force in response to cyberattacks, which could result in unintentional conflict escalation.

The Nature of Cyberspace

Cyberspace is a global domain where all actors connect, physically and virtually, through the cyber domain's infrastructure. The cyberspace environment enables billions of users, from individual actors and non-state organizations to states and multinational agencies representing various governments' interests on the global scene, to create virtual links from anywhere around the globe. Since 1995, the number of internet users has increased exponentially to over 3.4 billion; that equates to 46.1% of the global population.[5] The interconnectedness and scope of use among organizations and individuals around the globe creates potential ungoverned access points to a network's infrastructure for state and non-state actors alike that are susceptible to exploitation. These vulnerabilities allow actors at all levels to initiate a cyberattack from anywhere in the world and achieve results within milliseconds of pressing a button.[6]

---

[5] Internet Live Stats, "Internet Users," *Internet Live Stats*, last modified July 1, 2016, accessed December 12, 2017, http://www.internetlivestats.com/internet-users/.

[6] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 302.

A state has the ability to mitigate or stop most malicious actions originating from within its territory that target the state's population. However, a state is less likely to be able to affect cyberspace operations originating outside of its sovereign territory for two reasons: prohibitions against states interfering within the territory of other states and the lack of an internationally agreed-upon framework for responding to cyberattacks. The first reason is based on a mutual understanding and international agreements between states. The second reason is based on a missing bridge that facilitates states' coordination to allow for a response across state borders. This restriction contributes to the frustration of governments who are limited in their ability to fully govern and manage cyberspace operations intruding into their national infrastructure because actors determined to conduct illicit or aggressive behavior can operate remotely outside of the physical jurisdiction of the targeted nation.

The lack of internationally recognized standards of behavior to respond to or prevent cyberattacks favors ungoverned or potentially harmful activity intended to cross national boundaries by actors capable of taking advantage of the limited reach of states into other sovereign nations. This situation is exacerbated by the reality that states uphold and implement different standards of behavior. This allows actors to select a base of operations, or safe haven, outside of the target government that does not limit their activity into other domains with stricter laws governing cyberspace activity.

Finally, the cyber domain user population continues to grow while the level of knowledge to access cyberspace decreases. This reality is producing an abundance of potential for bad behavior. The internet is adding more users and connecting into more isolated regions of the globe at a pace faster than states' ability to develop and implement shared norms of behavior designed to stabilize relationships and security protocols among states.[7] In addition, as seen in

[7] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 30.

Figure 1, the speed of development and complexity of cyberattack capabilities is increasing while the technological savvy of the actor employing the increasingly sophisticated malicious software has exponentially decreased. In other words, an actor seeking to influence states or other organizations at any level no longer requires high levels of education and training to act. Rather, they only require access to predesigned software that can be used with the simple click of the mouse.

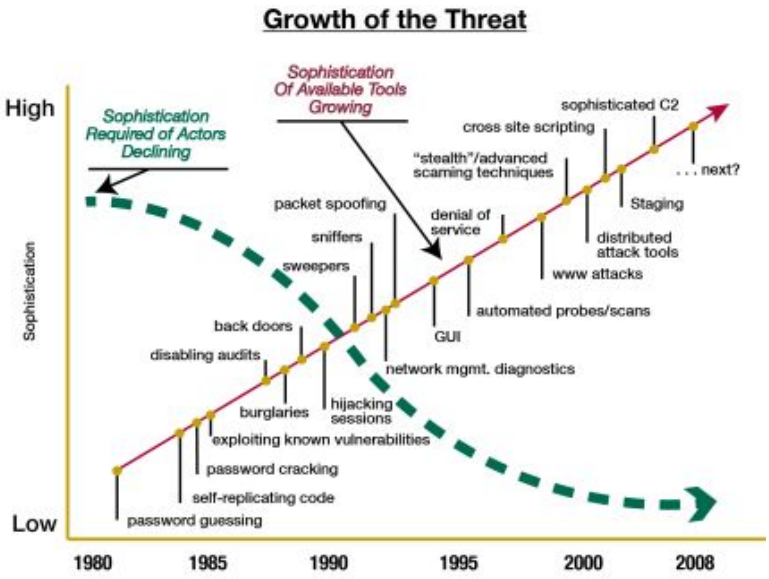

Figure 1. Growth of the Threat. Neil Robinson, "NATO: changing gear on cyber defence," NATO Review, accessed January 14, 2018, http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm.

Further, the complexity of the advances in cyberspace technology, such as artificial intelligence and ransomware, continue to put states' efforts to establish norms behind the power curve in their ability to moderate actors' responses to cyberattacks because politicians are generating options designed for outdated actions.[8] Successfully influencing the behavior of state and non-state actors allows an amount of predictability of action and intent when deciphering

[8] Debbie Garside, "Cybersecurity Trends for 2018," *Chief of Security Officer (CSO) Online*, last modified December 8, 2017, accessed January 14, 2018, https://www.csoonline.com/article/3241122/cyber-attacks-espionage/cybersecurity-trends-for-2018.html.

states' response to a cyberattack. Additionally, this predictability has the potential of creating a stable environment and avoiding overreactions by states to cyberattacks.

On the other hand, a government's inability to generate behavioral norms at a pace coincident with the pace of cyberspace capabilities development creates an environment that favors offensive actions in response to provocation.[9] This scenario played out in 2007 when Estonia was subject to a distributed denial of service (DDoS) cyberattack. In this situation, an Estonian government official likened the cyberattack as an attempt to "take one country back to the cave, back to the Stone Age" with the widespread deactivation of government, bank, and political party networks.[10] In response, Estonia petitioned the North Atlantic Treaty Organization (NATO) to respond with the use of conventional force under the provisions of Article 5 of the NATO Charter by equating the DDoS as an act similar to blockades of air and naval ports.[11] While NATO declined to initiate an armed response to a cyberattack due to issues of attribution and no clear definition equating a cyberattack to an armed attack, it highlights the possibility for an individual state to overreact and pursue an armed response when confronted with a cyberattack they are unable to stop.

Combined, the cyberspace qualities of global interconnectedness, a limited ability of states to influence actors outside of their sphere of influence, and an accelerated growth and expansion of cyberspace across the globe reduces trust and increases the risk of degrading international relations. This effect results from the circumstance where a state's cyber security is affected by another state's ability to make less stringent laws and enforce them with regard to cyber. This potentially increases the risk of armed conflict between actors where one is unable or

---

[9] Richard Hill, "Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT," *Cyber Conflict (CyCon): 2015 7th International Conference on Architectures in Cyberspace* (Summer 2015): 25, accessed September 28, 2017, http://ieeexplore.ieee.org/abstract/document/7158473/.

[10] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 306.

[11] Ibid.

unwilling to limit cyberspace operations and the other must suffer the consequences. Given Estonia's desire to react immediately based on inconclusive evidence, it is possible for an actor to conduct cyberattacks from a remote nation and for the actor's host nation to receive the blame for the cyberattack rather than the actor.

Cyberspace Risk

The nature of cyberspace establishes two primary risks that should be addressed in order to mitigate the threat to states' cybersecurity and national defense. The first is that the borderless and omnipresent nature of cyberspace provides the opportunity for an actor to choose an operating location that, because of the different standards and regulations of the intended target, provides a level of protection from retribution. International standards govern cross-border trade of globally traded commodities based on the ability of states to physically inspect, touch, and refuse entry to items that do not meet the standards of the destination. The nature of cyberspace creates an overwhelming volume of traffic that states are unable or unwilling to inspect one hundred percent of the transmitted data. This traffic flow in turn creates blind spots within states' inspection and review processes, which leads to the formation of safe havens for bad actors to exploit. This situation highlights the premise that creating safe havens is both a part of the nature and a risk of cyberspace.[12]

While cyberspace's global interconnectedness links the actor with the target, it is the creation of safe havens that creates risk for states because there are limited mechanisms in place to coordinate between countries for responding to cyberattacks. The lack of standardization and predictable responses in cyberspace encourages actors to risk aggressive activity because of the

[12] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," *Science, Technology, and Public Policy Program: Explorations in Cyber International Relations Project* (2011): 8, accessed November 26, 2017, https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf.

relative safety from international or cross-border retribution.[13] As a result, the ungoverned spaces in the cyber domain will continue to provide safety to attackers until states close legislative loopholes and agree to coordinate reactions to cyberattacks based on an agreed-upon set of norms.

A second risk is the relative autonomy with which private investors and organizations are able to determine their own level of cybersecurity and response to cyberattacks. This has significant implications for the risks to the international cyber community. Internet server and other components' physical locations determine how an infrastructure's administrator or owner applies security standards and accepted options available to respond to provocations. The concern is a lack of transparency between government and private industry that reduces predictability and increases the potential that an industry's actions will be attributable to a state and further escalate the situation. In November 2014, Sony pictures experienced a cyberattack resulting in the release of private and protected communication between the company's employees. It was speculated North Korea was responsible for the attack, but publicly shared evidence was inconclusive. Subsequently, North Korea experienced an internet outage lasting several days with no known attributable source for the interruption in service.[14] Whether North Korea's internet service interruption was a coordinated response or an independent reaction, it is likely the United States would have to deal with the fallout of any North Korean response.

Conversely, security standards and response options have potential to accelerate attribution determination by establishing trends and expected actions by friendly actors to distinguish them from cyberattacks. The difficulty and limited ability of states to regulate actions outside of their sovereign borders coupled with the lack of accepted response options reduces

---

[13] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 11.

[14] Lori Grisham, "Timeline: North Korea and the Sony Pictures Hack," *USA Today*, last modified January 5, 2015, accessed March 25, 2018, https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

predictability between actors and has the potential to create tension and mistrust between governments and private investors.[15] Additionally, in some instances, a state has limited ability to compel private investors to apply the government's standards on non-federally owned property.[16] Because all actors are linked to the global cyber domain, and states employ and enforce different standards for responding to and preventing a cyberattack, a private investor acting according to the standards of the country where they are located accepts risk for the cyber domain writ large, not just for themselves. The inconsistent application of responses to cyberattacks and security standards combined with the existence of safe havens for malicious non-state actors has had dramatic effects on the overall stability and security of cyberspace and increased the possibility of an overreaction that leads to an escalation of conflict.

Cyberspace Effects

The international community's variable application of behavioral standards in cyberspace make cyberspace an appealing medium for non-state actors to use to conduct cyberattacks for retribution or personal gain because of the low probability that a targeted state will respond across international borders. Cyberspace's nature and risk reinforce each other to cause effects that, in turn, have the potential to add tension between states and lead to conflict escalation. This is due in part to a state's uncertainty regarding the intent or gravity of an actor's operations in cyberspace.

In an age where nearly half of the global population connects to the cyber domain, non-state actors are able to operate with the same capabilities as a state but with less oversight. Additionally, because states provide nearly free and open access to cyberspace and the distinctions between military and civilian uses are often blurred, individual or small group actors

---

[15] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 15.

[16] Patricia Ladnier, "Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks," 33-34.

have the potential to wield similar capabilities and influence in cyberspace as states.[17] When combined with the difficulty of attributing responsibility or determining intent, states tend to err on the side of caution and assume a malicious intent when they are the subject of offensive cyberspace operations.[18] This tendency is reinforced by the difficulty of attributing and determining the scope or intent of the cyberattack which can range from a simple effort to collect data to an intentional disruption of a power-grid as happened in Ukraine in 2015.[19] When combined with the difficulty of attributing cyberattacks, the uncertainty of the intent and scope of the cyberattack, the prevalence of actors, and the limited technical sophistication needed to consistently attack from cyberspace, the ability of individual actors to engage national governments directly sets the condition for any actor to pose as, or operate on behalf of, a state and threaten the stability of relations between national governments. Because of this possibility, it is possible that states will consider lowering their decision threshold for using an armed response to a cyberattack. This highlights the need for a set of behavioral norms that establish a baseline for acceptable responses to provocations from actors in cyberspace so that states will be able to react to cyberattacks quickly with internationally sanctioned actions.

While some bilateral and regional organizations have drafted and adopted behavioral standards for response to cyberattacks, the multilateral cyber community, consisting of states and organizations around the globe, does not have a similar set of agreed-upon norms. For instance, two globally recognized standards, the Budapest Convention, which focuses on cybercrime, and

---

[17] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, vii.

[18] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, viii; US Department of Defense, Joint Publication (JP) 3-12(R), Cyberspace Operations (Washington, DC: Government Printing Office: 2013), GL-4, accessed August 15, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. Offensive cyberspace operations defined as "cyberspace operations intended to project power by the application of force in or through cyberspace."

[19] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law; Washington* 110, no. 3 (July 2016): 434, accessed November 3, 2017, https://search.proquest.com/docview/1830058161/abstract/4612A6ADBDB44F13PQ/1.

the Tallinn Manual, which focuses on international law related to cyberspace, do not provide criteria a state might consider when determining the appropriate response to a cyberattack.[20] For instance, NATO, as a multilateral, regional alliance, is making attempts to clarify its opinion on the type of cyberattack that warrants a military response and subsequently announced its position that a cyberattack against an alliance member could be considered a reason for initiating Article 5 military operations.[21] The relevance is that increasing tension, instability, and unpredictability builds apprehension between countries. States unsure if an actor is attacking them or probing for advantage will favor an aggressive response if they suspect a threat to their perceived asymmetric advantage in technology and zero-day vulnerabilities that have a limited shelf-life. NATO's policy change to consider Article 5 actions reflects a growing sense of uncertainty regarding the alliance's perception of vulnerability and subsequent growing acceptance of armed conflict to maintain its security.[22]

When faced with an adversary of unknown capability in cyberspace, a state will favor action to preserve its perceived asymmetric advantage.[23] Together, the difficulty of finding internationally agreed-upon standards for employing conventional military forces in response to a cyberattack in conjunction with a lower decision threshold for offensively responding to these threats sets the conditions where a state is likely to consider an aggressive response to a cyberattack if it perceives a threat to its security and military advantages.

---

[20] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 25.

[21] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 297-8.

[22] Asymmetric advantages are the capabilities believed by states to increase their ability to breach an adversary's cyber defenses or withstand an adversary's attempts to defeat its own cyber defenses. In this instance, a state perceives the balance of power is in their favor and will make decisions to preserve the advantage when faced with an unknown actor or cyberattack that threatens the state's advantage.

[23] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 28.

Similarly, the speed with which cyberspace adapts and modernizes increases concern that states will favor escalating tensions diplomatically, economically, or militarily to avoid being outmatched. "In terms of classical strategic analysis, the 'ways' of cyber warfare are such that 'crisis instability' and 'arms race instability' might ensue."[24] In the case of crisis instability, states will likely preemptively act before a cyberattack and in a timeframe earlier than other states would expect due to the government's growing insecurity about maintaining a perceived technological advantage, both offensive and defensive, over an adversary.[25] The perception and uncertainty associated with the capabilities of powerful states can lead to unintended consequences including arms races and armed conflict. Without standards of behavior for responding to cyberattacks, aggressive cyberspace capabilities used by the Russian Federation in 2007 and 2008 against Estonia and Georgia as well as alleged actions by the United States in 2010 against Iran will continue. This scenario will lead to increased tension and instability between states and the likelihood that governments will accelerate their acquisition of advanced cyberwarfare capabilities to mitigate any advantages of an adversary.

Further, the uncertainty caused by the lack of clear standards is likely to cause tension between government and private industry actors. Without clear standards for responding to cyberattacks, state and private industry actors lack a foundation to build trust and transparency by managing expectations of how each works in cyberspace. The increased strain caused by this circumstance results from a government favoring security over freedom of access and privacy. Favoring one interest over the other, in turn, reinforces a difference of opinion between the government (security-focused) and private industry (freedom-of-access-and-privacy focused) with respect to an acceptable use of cyber domain capabilities when dealing with cyberattacks.[26]

---

[24] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 29.

[25] Ibid., 29-30.

[26] Igor Mikolic-Torreira, *A Framework for Exploring Cybersecurity Policy Options*, Research Report, RR-1700-WFHF, Santa Monica, CA: RAND, 2016, 12-17.

Favoring security will often reduce access and privacy. The reverse is also true. States and industry rely on each other to develop capabilities and ensure the security of the state and its population. If there is tension or a lack of trust, both are at risk and less likely to maintain advantages in cyberspace. When the interests of security and access are unbalanced, the situation opens the state to potential vulnerabilities in the cyber domain.

The government's response to a terrorist attack in California in 2016 highlights this difference and the need to strike a balance between the two views. As part of the investigation into the terrorist shooting in San Bernardino, California in 2016, the Federal Bureau of Investigation requested Apple to break into its own software to download information from the terrorists' mobile devices with the intent of identifying the existence of a wider network of terrorists. The ensuing debate highlighted the imbalance of interests when responding to the situation and the absence of trust between the state and private industry.[27] The state desired access to private information as part of an investigation, but the private industry feared such access was too high a risk to the privacy of the public's personal information. It is possible that a set of agreed-upon standards could have provided a precedent built on understanding and trust to achieve the interests of both the state and private industry.

These risks, when ungoverned and allowed to develop, have specific effects both actual and perceived that negatively influence international relationships between states and non-state actors. There are too many varied capabilities designed to take advantage of the cyberspace domain and there is no panacea defense capable of safeguarding a state against all forms of cyberattack. States should view the situation from a different perspective and focus on behavior and action to influence and stabilize international relationships rather than a continuous search for

[27] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," 425-6.

a temporary offensive or defensive silver bullet.[28] In other words, states should seek a long-term agreement that influences the behavior of how states respond to cyberattacks rather than searching for a means to maintain an elusive asymmetric advantage in cyberspace.

Increased cooperation, information sharing, and an agreed-upon set of behavioral norms have the potential to reduce the uncertainty and raise the threshold for military action while simultaneously lowering the threshold for a non-military solution. Establishing standards and norms is a method to establish a shared understanding of cyber behavior and reduce the potential for conflict escalation by avoiding overreaction or misinterpretation of actions as hostile or offensive.[29] To alleviate the dangers of this scenario, states should pursue a means conducive to developing and approving a set of response norms in the cyberspace environment.

International Standards for Responding to Provocations Are Necessary

According to Randall Dipert, C.S. Peirce Professor of American Philosophy at the University of Buffalo, the ontology of cyberspace does not conform to established legal regimes based on "well-defined physical locations, clearly delineated geographical boundaries, and concrete personal property or state territory."[30] Existing legal precedents and standards using these physical attributes are not applicable when discussing actions and reactions in cyberspace because of cyberspace's ill-defined, diverse physical infrastructure, porous boundaries, and the uncertain ownership of states' jurisdiction over cyberspace. In order for a state to protect and strengthen its national security and reinforce a global network of responsible actors within cyberspace, it is critical that governments cooperate with the development and adoption of

---

[28] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," 435-6.

[29] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 31.

[30] George R. Lucas, Jr., "Emerging Norms for Cyberwarfare," in *Binary Bullets: The Ethics of Cyberwarfare*, ed. Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (New York: Oxford University Press, 2016), 15.

"norms of responsible behavior" when responding to cyberattacks, which are designed to mitigate the risks and effects associated with the nature of cyberspace discussed previously.[31]

Norms, defined as "agreed-upon rules of behavior that will ideally reduce the possibilities of disproportionate response and conflict escalation in cyberspace," offer two advantages that make them ideal for consideration as a solution to mitigating the risks and effects of cyberspace.[32] First, through a common framework, language, and understanding of standards of behavior or set of expectations, it is possible for states to operate at reduced levels of tension and anxiety about actors in cyberspace. Governments need a template, standards of behavior or set of expectations based on experience and prior knowledge of right and wrong, on which to compare their environment in order to determine whether a situation conforms to established norms. The standards and expectations link experience and prior knowledge to a state's environment and bring clarity to domains that are new or ill-defined.[33] States with little or no experience in cyberspace may not have the necessary background or expertise to interpret cyber activities accurately and may fall back on ill-suited analogies and associated responses that could lead to conflict. Without a frame of reference to guide states in their governance of cyberspace, there is a higher probability of governments interpreting actions through their own biased worldview instead of a shared, global lens, which could end in a disagreement and escalate into an armed conflict.

---

[31] US Department of Defense, "The Department of Defense (DoD) Cyber Strategy" (Washington, DC: Government Printing Office, 2016), 3-4, accessed August 21, 2017, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

[32] Emilio Iasiello, "What Happens if Cyber Norms are Agreed To?" *Georgetown Journal of International Affairs; Washington* 17, no. 3 (Fall 2016): 30, accessed October 1, 2017, https://search.proquest.com/docview/1924880335/abstract/A910C9778B9840C2PQ/1.

[33] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 10.

Governments have developed and implemented their own standards for acceptable responses to threats from cyberspace since the domain was created. According to the former Director of the Central Intelligence Agency, Michael Hayden, "Cyber was moving so fast that we were always in danger of building up precedent before we built up policy."[34] It is possible states will develop policy based on practice or trial and error rather than practice based on policy, which leads to a lack of understanding of the implications or consequences of reacting to cyberattacks. This has the potential to increase a state's misunderstanding of an actor's intent due to a lack of a shared worldview of acceptable responses to cyberattacks. It is necessary for individual governments to forego generating additional state-specific retaliation standards and commit their efforts to an international, global solution.[35] In this way, it is possible to lay the foundation for expectations of actors in cyberspace, which builds stability and trust and strengthens international relationships, the second advantage of standards and norms.

It is not necessary to witness a catastrophic cyberattack on a state's infrastructure or economy in order to develop and adopt standards for countering cyberthreats and limiting operations designed for cyber warfare. Similar to limitations on the use of other weapons of mass destruction or effect, there is a benefit to creating behavioral norms in cyberspace without the need to experience the results first-hand. This type of standard adds predictability to the cyber domain and legitimizes controlled escalation should an actor cross the threshold into unacceptable behavior.[36] In addition, an approved global solution provides options for states to enforce approved legal constraints internally via prescribed, legitimate reactions. This has the benefit of

---

[34] Ellen Nakashima, "Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies," *The Washington Post*, last modified March 19, 2010, accessed December 29, 2017, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html.

[35] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 23.

[36] Ibid., 3.

instituting a greater level of control by the government on actors' behavior within their sovereign territory according to a standard accepted by all nations.

Internationally agreed-upon standards of behavior create a baseline for states to use as a means to provide limits and guidance to actors in cyberspace. By adopting international standards and norms, governments provide legitimacy to its actions and decisions. This, in turn, provides a foundation on which to set their own enforcement policies, reinforce a global network of responsible actors, and reduce or eliminate loopholes used to create safe havens.[37] Additionally, establishing standards and norms improves cybersecurity by setting expected patterns of behavior, which creates an incentive for non-state actors to comply in order to avoid consequences.

The goal, therefore, is to determine the best means or process to develop and implement standards of behavior that are applicable to all actors, enforceable by states, and hold individual states accountable for employing the standards and norms. Conducting business through unilateral actions and decision along with governance through individual action to achieve standards of behavior will not work; a different method is required that shares cyberspace's characteristics of global interconnectedness and is capable of stabilizing relations between states. An alternative method of using state alliances focuses on a system with experience generating norms between governments.

Alliances Are the Answer

Alliances seeking to develop and adopt international standards and norms exhibit certain characteristics that increase the likelihood of success. These characteristics include political control, inclusivity, and institutional authority to enforce decisions. First, political control means that the membership of the alliance consists of individuals appointed politically by a state to

[37] George R. Lucas, Jr., "Emerging Norms for Cyberwarfare," 18-19.

represent and serve that government's national interests.[38] As stated in a Chatham House Royal Institute of International Affairs report, technical experts are necessary to formulate the details, but political leaders are essential to provide the strategic guidance and views to ensure applicability across states and environments.[39] Second, inclusivity describes a process that seeks out and incorporates several points of view, often differing, before reaching a decision. A set of acceptable standards will require close collaboration between states and private industry to ensure that all stakeholders have a voice in the norm generation process.[40] Third, institutional authority implies that the members will abide by the decisions of the alliance based on signed agreements or other binding documents. This aspect is necessary to enforce guidance that reflects a compromise rather than full support to any one idea or proposal. In the case of the cyber domain, any proposed baseline response to cyberattacks should balance the competing interests of the security and the freedom of access and privacy of actors.[41] These characteristics of an alliance are necessary to overcome the limitations of an individual state's ability to enforce international standards outside of its sovereign territory.

The decision of how to respond to a cyberattack is a political decision, because a military response is not always appropriate. In general, offensive application of national capabilities as weapons belong in the realm of political control because of the potential for widespread and devastating effects. Further, political leaders or their representatives have a general understanding of the relationship and effects of cyberspace capabilities and their implications on policy and

---

[38] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 1-2.

[39] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 19.

[40] US Department of Defense, "The Department of Defense (DoD) Cyber Strategy," 4, 7-8.

[41] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 1-2.

norm development in order to work effectively within an alliance.[42] In this way, it is political control that provides the best perspective and balance for using cyberwarfare operations. Therefore, emphasizing political control of these operations when responding to cyberattacks as a behavioral standard brings stability to the domain. Further, ensuring political control within an alliance structure imbues any prescribed standard with the values, morals, and interests of the alliance and its member nations. Normalizing the decision process to use cyberwarfare operations requires an effort to characterize any cyberattack as a military or criminal act before applying a response. This increases the likelihood that a state's courts are as likely as the military department to respond to a cyberattack because not all provocations, once characterized, will warrant a military response.[43]

Therefore it is crucial for an alliance tasked with developing and adopting norms that provide a baseline for acceptable responses to cyberattacks to employ a state's political leaders and representatives as members of the decision-making process.[44] This action provides the benefit of ensuring political control and consideration of offensive cyber operations and accelerating the decision-making process because political leaders and their representatives have authority to bind or commit their state to a course of action. Further, the technical aspects of the cyber domain make cyberspace experts unlikely candidates to lead efforts in standardizing responses because of a likelihood that they would focus on the details rather than the big picture. Instead, political leaders should lead the effort with the assistance and advice of the experts.[45] This keeps discussions at the strategic level and avoids delving into details that would defeat the intent to create an international standard applicable to all cyberspace actors. This further deescalates

---

[42] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 1-2.

[43] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 2-6.

[44] Ibid., 18.

[45] Ibid., 19.

tension among states by exercising government control over the use of offensive cyberspace capabilities based on shared response expectations.

Second, attempts to build standards for acceptable responses to offensive cyberspace operations must be inclusive of all aspects of the domain and its actors because of the diverse interests related to a state's security and defense.[46] Alliances, by their nature, incorporate multiple states with the advice and opinion of independent organizations and technical experts as part of their normal processes and are an ideal venue to accomplish the task of formalizing norms. The benefit of inclusivity within an alliance, as it relates to the cyber domain, is the opportunity to incorporate advice and knowledge from both state representatives and private sector experts in order to create a set of standards and norms acceptable to all stakeholders. Additionally, as an alliance grows in membership by seeking diverse representatives and opinions and emphasizes robust discourse prior to a decision, it will increase the probability of buy-in and implementation. This will allow states to realize a form of collective control leading to increased stability and reduced tension among the alliance's members.[47] This is in line with Finnemore and Hollis's norm generation theory for norm development, which emphasizes the criticality of socializing desired end states and preferred solutions among peers and trusted allies prior to making a decision in order to build agreement that empowers the outcome with legitimacy.[48]

Finally, an alliance should have institutional authority to influence and enforce the decisions of the organization among the member states. Alliances operate with a power and influence representative of the organization rather than a reflection of any one member. In this way, they reflect a consensus that has a stronger power and momentum to convince member

---

[46] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 1-2.

[47] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," 460.

[48] Ibid., 429.

states to accept agreed-upon decisions.[49] Further, an alliance should have institutional authority to leverage this power and momentum. With respect to cyberspace, this is necessary because of the competing interests of security and freedom of access and privacy, each prioritized differently by states, that will shape any baseline standards for countering aggressive behavior in cyberspace.[50] Additionally, institutional authority takes advantage of the member states' established trust relationships and inclination to observe and emulate one another to convince governments to conform with the alliance's decisions. When applied to states developing more sophisticated cyberspace infrastructure and capability, it is likely they will adopt common practices and standards as part of an international agreement because of a tendency to conform and a desire to maintain any perceived advantage or overcome any sensed inadequacy.[51] In this environment, the best vehicle to develop and implement an agreed-upon set of international standards and norms for state actors is an established, international alliance that operates with political control, maximizes the inclusivity of states and private interests, and demonstrates a capability to enforce the alliance's decisions.

Alliance Options from the Ground Up

Alliances are a preferred forum to develop and apply international standards and norms to influence the extent and scope of individual states acting to protect perceived vulnerabilities. International standards and norms that provide a baseline for acceptable responses to cyberattacks balance the playing field, reinforce stability, and reduce tension by creating predictability and

---

[49] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 9.

[50] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 1-2.

[51] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance; Boulder* 18, no. 3 (September 2012): 350, accessed October 2, 2017, https://search.proquest.com/docview/1034977196/abstract/AF19564F3E9C4595PQ/1.

enforcing the same standards and expectations among states.[52] In today's international community, bilateral alliances between states with significant international power and influence are able to set trends and decrease suspicion between governments by deliberately sharing information and working closely to ensure transparency during operations involving cyberspace. Multilateral alliances, on the other hand, enjoy an increase in collective security, but tend to focus on either organized military or criminal defensive measures with respect to the cyber domain. Between these two alliance alternatives, there are several functional alliances composed of governmental study groups or agencies whose purpose is to analyze and recommend solutions to the larger alliance structure's cyberspace concerns. Together, these alliances have developed viable behavioral norms in cyberspace, but because of their lack of political control, inclusivity, or institutional authority, they are incapable of setting a baseline for standards of behavior in the cyber domain and, consequently, unlikely to have a global effect and mitigate the risks and effects of cyberspace that have the potential to lead to an unintended escalation of conflict.[53]

Bilateral Alliances

Generally, bilateral alliances tend to have a specified purpose and desired outcome. Governments tend to enter bilateral alliances with the intent of reducing tension within an existing adversarial relationship or increasing the alliance's power and influence within a community. The United States and China continue to participate in Defense Consultative Talks with the express purpose of "bringing greater understanding and transparency of each nation's military doctrine, policy, roles and missions in cyberspace. The goal of this work is to reduce the risks of misperception and miscalculation that could contribute to escalation and instability."[54] As

---

[52] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," special expanded issue, *The Tallinn Papers*, no. 5 (2014): 19, accessed October 2, 2017, http://www.ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf.

[53] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," 466.

[54] US Department of Defense, "The Department of Defense (DoD) Cyber Strategy," 28.

traditional competitors in cyberspace, these states recognize the need to increase communication between their governments in order to build a common set of standards of behavior for the purpose of stability.

Conversely, the United States and the United Kingdom, considered superpowers in cyberspace, are able to reinforce their security and capabilities by working in synch to coordinate their responses.[55] Their close cooperation and information sharing enhances both their offensive and defensive cyberspace capabilities and strengthens their overall presence in the cyber domain. Similarly, states within the African Union bilaterally negotiate behavioral standards and cooperative response actions between neighboring governments.[56] Without a mature alliance including more than two nations on the continent of Africa, individual states must adopt bilateral agreements for the purpose of building their cyberspace capabilities and strengthening their security against exploitation. These bilateral agreements are beneficial to those governments participating in the alliance but lack the inclusivity and institutional authority to influence states on a global scale.

Multilateral, Regional Alliances

On a larger scale, multilateral, regional alliances amplify the benefits of bilateral alliances. Additionally, these alliances tend to focus their cyberspace response efforts on either prioritizing military or civilian legal measures to the near exclusion of the other. As one of the largest multilateral, regional alliances, NATO embraced the need to generate and approve standards of behavior in cyberspace in order to reinforce its collective defense and military response to cyberattacks. Specifically, in September 2014, NATO acknowledged for the first time

---

[55] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, viii, 17.

[56] Uchenna Jerome Orji, "Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?" *Cyber Conflict (CyCon): 2015 7th International Conference on Architectures in Cyberspace* (Summer 2015): 111-3, accessed September 28, 2017, http://ieeexplore.ieee.org/abstract/document/7158472/.

that a cyberattack could result in a military response according to Article 5 of the North Atlantic Charter.[57] NATO codified this and other expectations and standards in its Cyber Defence Policy, which coordinates actions and establishes a combined response during any provocation in cyberspace based on an acknowledgement that a multilateral approach is necessary and preferred to any individual member nation acting alone.[58] This new policy is significant because it lays a foundation that allows non-alliance members to determine how NATO will respond if provoked. This action removes some level of uncertainty for actors in the cyber domain regarding NATO's intentions and protocol for responding to cyberattacks. It also reduces the threat of armed conflict or cyberwarfare because there is a shared expectation of consequences for actions against members of the alliance.

Another multilateral, regional alliance of significance is the European Union (EU), which focuses on a criminal defense of the alliance using law enforcement versus the military. Unlike NATO, one of the EU's primary functions is the control and governance of the commercial sectors across the alliance and the guarantee of protection and prosperity for all members. To that end, the EU Cyber Security Strategy "is based on promoting norms in cyberspace, encouraging dialogue between nations, enhancing technical capacity and resilience, and fighting cybercrime."[59] In furtherance of the alliance's emphasis on government and industry cooperation in the cyber domain, the alliance incorporates actors from both sectors as representatives in various partnerships such as the European Public-Private Partnership for Resilience and Trust in Digital Life to increase internet security and establish stronger legal enforcement programs.[60]

---

[57] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 297-8.

[58] Ibid., 307.

[59] Ibid., 311-2.

[60] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 19.

These multilateral, regional alliances, NATO and the EU, provide the necessary capabilities of political leadership, regional inclusivity, and institutional authority to successfully generate and implement standards of behavior in cyberspace. Similar to bilateral alliances, though, multilateral, regional alliances have a limited membership that lacks a global inclusivity needed to ensure a worldwide influence. In the case of NATO and the EU, key states involved in the cyber domain, namely the Russian Federation and China, are not involved and, in the case of NATO, are the primary focus of the alliance's defense strategy.

Functional Alliances

A third type of alliance designed to provide functional support to bilateral and multilateral alliances is a functional alliance that includes multinational political leaders with study groups and technical experts as advisors who provide analysis and recommendations for the security, stability, and governance of the cyber domain. The United Nations and NATO have organized various functional alliances such as the International Telecommunications Union (ITU), Internet Governance Forum, and Cooperative Cyber Defence Center of Excellence as a first step towards establishing standards of behavior and incorporating applicable international law to create a baseline for norms and expectations among member states.[61] An implied expectation of the parent organization is that the functional alliance will provide an unbiased recommendation on an issue. However, a consequence of the alliances' links to their parent organization is that the alliance has a tendency for member states to attempt to influence and sway the findings of the functional alliances towards their own individual government's interests which dilutes the functional alliance's ability to develop the best recommendation regardless of individual states' interests.[62] The subordination of the functional alliance to a parent organization

[61] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," 4, 30.

[62] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," 346.

is the reason the functional members cannot exert the political control or institutional authority necessary to globally affect change in international behavior in cyberspace. Further, functional alliances share the same general lack of global inclusivity of bilateral and regional alliances due to their subordinate relationship to the parent alliance and their inability to incorporate relationships with states that may be hostile to the parent alliance.

Cyberspace requires additional behavioral norms that existing bilateral and regional alliances, treaties, and diplomatic agreements, such as the Budapest Convention, do not provide. While standards and norms regarding cyberspace behavior exist, states and international organizations express a need for more that encompass the global community rather than just bilateral or regional interests. It is incumbent on the international community to leverage existing trust relationships within a global alliance for the purpose of developing and approving behavioral standards that address these issues affecting the international cyberspace community.[63] State representatives and cyberspace experts from the private and commercial industries supported this premise at the 2013 Seoul Conference on Cyberspace and East West Institutes 2012 Cybersecurity Summit "noting: 'securing cyberspace is a global challenge–one that cannot be solved by a single company or country on its own."[64] It is important states appreciate the reality that unilateral, bilateral, or regional solutions cannot resolve global concerns. States must elevate their focus and efforts to the global stage to successfully influence the international community.

The issues presented are global and interconnected. Any solution should be equally global and interconnected to achieve international standards that meet global interests rather than

---

[63] Markus Maybaum and Jens Tölle, "Arms Control in Cyberspace-Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods," *Cyber Conflict (CyCon): 2016 8th International Conference on Cyber Power* (Summer 2016): 168, accessed September 28, 2017, http://ieeexplore.ieee.org/abstract/document/7529433/.

[64] Richard Hill, "Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT," 121-2.

only individual, bilateral, or regional interests. It is necessary, then, to find a multilateral, global alliance that incorporates political leaders from the around the globe, incorporates all parties with interests and expertise in cyberspace, and has institutional authority mechanisms in place to enforce decisions made by the organization. The answer is simple, and states must look no further than the United Nations.

Quest for a Silver Bullet

To date, standards and behavioral norms generated by individual, bilateral, and multilateral, regional alliances to provide a baseline for acceptable responses to cyberattacks are not coordinated globally and represent numerous disparate attempts to mitigate the risks and effects of the cyberspace domain. As a result, there are doubts that the norms are sustainable given the ability of state and non-state actors to exploit the loopholes created by competing policies.[65] Therefore, it is likely that a state will choose to act decisively and with overwhelming force if it perceives that the threat warrants such a response when there are no standards for the state to consider before reacting to cyberattacks. It is incumbent, then, that the international community cooperate as an alliance to bring together the necessary leadership and expertise to develop and implement a global solution. Many states and other actors do not disagree about the need for behavioral norms to standardize an actor's responses to provocations, but it is the type of alliance used to bring forward the standards of behavior that is in doubt. This section will explore reasons against and for the United Nations as the preferred alliance to develop and implement standards and then conclude with ongoing efforts that are creating momentum within the international community to achieve global stability.

---

[65] Richard Hill, "Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT," 126.

There Is No Panacea

Those opposed to multilateral, global alliances taking the lead in the development and implementation of international behavioral norms cite three reasons for this belief. First, the United Nations has 193 member nations unwilling to compromise their national interests and support a common goal of stability in cyberspace. Second, the commercial sectors should lead any development and implementation of international standards of behavior in cyberspace because they have more experience in the domain and exert greater authority over the cyberspace infrastructure.[66] Finally, an alliance of this size lacks the authority to unequivocally bind and enforce application of an agreed-upon set of standards.[67]

Global alliances struggle to establish and adopt global, international standards and norms in cyberspace because individual states have a tendency to advocate for their individual national interests and desired end state tenaciously to the exclusion of possible shared global interests. As a result, individual nations join alliances that share their common interests and methods to achieve their desired end states. For example, states join NATO and the EU based on the organizations' desired interests and end states. NATO desires a military response to strengthen its cybersecurity and defense while the EU favors police actions that emphasize its desire to fortify its cyber security in the commercial and industrial sectors. Additionally, states in general appreciate the positive benefits of international standards for responding to cyberattacks. However, western democratic governments are apprehensive of the possibility of authoritarian states using the standards to justify censorship and restrict access to its citizens by exerting unilateral control of access, content, and use of cyberspace under the auspices of implementing

---

[66] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 26.

[67] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 340.

the standards for national security.[68] This results in lengthy debates and negotiations, leaving the impression that the political leaders will not be able to resolve their differences in order to reach a decision.

However, in 1998, the Russian Federation first introduced a code of conduct for cyberspace to the United Nations General Assembly. This was swiftly defeated for the reasons listed previously, but, undeterred, the Russian Federation introduced its draft resolution every year since, which resulted in an increasing number of alliance members agreeing to support the resolution in 2006. Critically, the United States removed its block of the resolution in 2010 after recognizing a growing momentum among other states to approve the document and realizing its opportunity to participate and influence the final resolution and accompanying standards of behavior was quickly disappearing.[69] Satisfying the concerns of how different states would apply the international standards seems daunting. Successful negotiations will require a concerted effort by the alliance members to concentrate on the shared interests of freedom of access and privacy and security rather than the potential for malicious actors to conduct offensive or criminal operations.[70] The United Nations has a 72-year history of repeated success in adopting global resolutions that are a compromise, are inclusive, and allow equal participation from all nations during the negotiation process. The growing momentum over the previous two decades to approve the Russian Federation's draft cyberspace code of conduct shows the viability of the United Nations as a multilateral, global alliance capable of achieving meaningful success.

---

[68] Richard Hill, "Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT," 123; Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 4.

[69] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 25-6.

[70] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 1.

A second critique of multilateral, global alliances leading efforts to develop and adopt standards for cyberspace is that the private industry is better equipped to define acceptable standards because it has a preponderance of technical expertise and knowledge of the cyber domain. The private sector often owns or operates most of a nation's cyberspace infrastructure and its lack of official representation as a voting member at the United Nations implies that there is a commercial aspect not being considered within alliances because of states prioritizing national security.[71] Ultimately, private sector advocates believe that since the sector employs the majority of technical experts and professionals in cyberspace, regularly defends against and responds to cyberattacks, sustains international business relationships, and manages the lion's share of a nation's critical cyberspace infrastructure, it is capable of establishing and better equipped to establish standards for actors in the cyber domain.[72]

While the premise is clear that the private industry should lead the task of drafting and approving standards for cyberspace actions, it is the sector's focus on its financial interests in cyberspace that invalidates this claim. As mentioned previously, states view the cyber domain and its infrastructure as a matter of national security. Conversely, because private and foreign investors own and operate large portions of the critical cyberspace infrastructure as a business, their focus centers on their "bottom line" rather than a state's security concerns.[73] Consequently, decisions by the private industry based on financial risks rather than security risks create potential vulnerabilities for governments without coordination or consideration of the implied or actual security risks to the state. In fact, during the 1990s and at the recommendation of the private sector, the United States government enacted legislation to separate the government from internet

---

[71] US President, Executive Office of the President, "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" (Washington, DC: Government Printing Office, 2003), 8, accessed February 9, 2018, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf; Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 22.

[72] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 26.

[73] Ibid., 22.

oversight in order to preserve the "open commons" of the domain.[74] However, all of this was prior to the emergence of sophisticated, malicious, offensive cyberspace operations conducted by state and non-state actors. The growing intensity and regularity of threats to a state's national security from cyberspace no longer support the idea of private industry leaders dictating standards and norms based primarily on economic risks.[75] The increase in both the number and complexity of offensive operations from the cyber domain necessitates a multilateral, global alliance capable of acting from a broader, inclusive view that prioritizes security risks and concerns among all national interests.

Finally, multilateral alliances such as NATO, the EU, and ASEAN generally do not have the authority to mandate behavior and, lacking this capability, cannot enforce standards and norms. To successfully develop and adopt standards of behavior, the vehicle to do this must have power, perceived or legal, over actors in order to influence and change behavior.[76] The United Nations, as a multilateral, global alliance, utilizes the Security Council and General Assembly to bind states according to Article 25 and Articles 10 and 12 respectively. When the Security Council approves a resolution, it binds all member states to "accept and carry out" the mandate according to Article 25.[77] Conversely, when the General Assembly approves a resolution, it is a recommendation to all member states to consider accepting for implementation according to Articles 10 and 12.[78] These methods offer alliance members options for drafting and

---

[74] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," 342.

[75] Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," 343; Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization; Cambridge* 52, no. 4 (Autumn 1998): 899, accessed November 1, 2017, https://search-proquest-com.lumen.cgsccarl.com/docview/219221738?pqorigsite=summon.

[76] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 304.

[77] Chapter V: The Security Council Functions and Powers, June 26, 1945, *Charter of the United Nations*, accessed December 27, 2017, http://www.un.org/en/sections/un-charter/chapter-v/index.html.

[78] Chapter IV: The General Assembly Functions and Powers, June 26, 1945, *Charter of the United Nations*, accessed December 27, 2017, http://www.un.org/en/sections/un-charter/chapter-iv/index.html.

implementing cyberspace standards of behavior. The process is not foolproof but does provide a method to generate and approve behavioral norms on a scale unattainable by other alliances because of its legitimacy, acceptance, and wide membership.

This makes the United Nations the preferred venue to create and socialize behavioral norms in cyberspace because of its political nature and ability and desire to incorporate multiple opinions from disparate communities, not just states.[79] These qualities, combined, support the premise that the United Nations should direct the formation and adoption of standards for responding to cyberattacks.

Established Alliances Could Be the Key

The United Nations is the preferred venue to develop and implement standards of behavior in cyberspace because it meets the criteria necessary to achieve success: political control, inclusivity, and institutional authority. To begin, using the United Nations as the medium to develop and implement standards of behavior capitalizes on the importance of political control of operations in cyberspace. Because state and non-state actors can militarize cyberspace, it is necessary for political leaders to exert control of cyberspace operations by leading efforts to craft, adopt, and enforce standards for responding to cyberattacks. By doing so, they can ensure that the decision-making procedures used by the United Nations address all aspects of a state's national security, retain an ability to control offensive capabilities, and find shared interests to form the basis for standards and norms. By starting with a common framework and understanding of the issue, the political leaders are more likely to achieve consensus. Further, agreements formed and adopted at the United Nations have added legitimacy and international buy-in, which benefits states by creating shared expectations that limit non-state actors from malicious and illicit operations by closing loopholes and reducing the opportunity to find a safe haven.[80]

---

[79] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 33.

[80] Ibid., 23-24.

The "real power of norms (and much of their attraction as a regulatory tool) lies in the *process* by which they form and evolve," to include who sponsors the proposed norms, how the norms are approved, and who adopts them.[81] The ability to influence actors' behavior is predicated on the answers to these questions.[82] It is precisely for this reason the United Nations is the preferred medium to achieve this goal. Current United Nations initiatives seek to incorporate the private sectors as evidenced by their inclusion within sub-organizations' research into cyberspace solutions according to United Nations General Assembly Resolution 64/211.[83] This ensures international dialogue has a good chance of being acceptable to the alliance writ large and palatable to the global private industries.

Further, the United Nations offers a venue and process that is inclusive of all member nations, provides transparency among the members through open dialogue, and incorporates opportunities for all member states to voice their opinions for inclusion in the final product. The collaborative effort allows governments an opportunity to appreciate the interests and intent of partner states as the standards and norms are prepared and affords each state a chance to determine its acceptable level of risk based on the planning process and confidence in the standards' effect on their individual security. With respect to the cyber domain, individual state interests cannot be guarded in a vacuum. The actions of all actors affect the security of everyone and if dealt with collectively, there is a higher probability of reaching consensus, establishing behavioral norms that will strengthen the cyberspace community, and reduce the threat of bad actor safe havens and vulnerabilities across the domain. The United Nations is able to bring together states, technical experts, private and commercial industry leaders, and regional alliances to discuss issues and has the institutional authority and legitimacy through the previously

---

[81] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," 427.

[82] Ibid., 427-8.

[83] Patricia Ladnier, "Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks," 63-64.

mentioned United Nations Charter to implement both binding and non-binding decisions regarding the implementation of norms.

As an example of leveraging its political control, inclusivity, and institutional authority on a matter of international interest, the United Nations used its existing trust relationships and resolution adoption processes to successfully implement international standards and norms in the area of private security. In 2008, the Montreux Group petitioned the United Nations General Assembly to adopt the Montreux Document in order to promote respect and observance of international humanitarian law and human rights laws when states employ private military contractors and private security companies.[84] The group created and socialized an appealing and persuasive argument to support its recommendation based on examples of common law, best practices, and largely agreed-upon standards and norms as part of regular discussions among member nations' political leaders. Once the group was confident that it would receive consensus support from the United Nations members, it presented the document for vote at the United Nations General Assembly and obtained broad approval. As of 2017, fifty-four states and three multilateral, regional alliances have signed and implemented the document.[85] By incorporating political control, inclusivity, and institutional authority, the United Nations can succeed where other organizations have not.

Momentum Is Building

While there have been no approved and implemented international standards in the cyber domain related to acceptable responses to cyberattacks, the United Nations continues to make deliberate progress to that end. Through the use of suborganizations and the organization's

---

[84] George R. Lucas, Jr., "Emerging Norms for Cyberwarfare," 17-18.

[85] Federal Department of Foreign Affairs, "Participating States of the Montreux Document," *The Federal Council, the Portal of the Swiss Government*, last modified November 11, 2017, accessed February 10, 2018, https://www.eda.admin.ch/eda/en/home/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/participating-states.html.

established administrative processes, the alliance is setting the conditions for the eventual presentation and adoption of behavioral norms for the cyber domain.

The United Nations classifies discussions of cyberspace into two categories, political (security focus) and economic (criminal focus). Each category uses established or specified committees and suborganizations to develop and staff policy resolutions for the Security Council's and General Assembly's consideration.[86] The efforts of the committees provide a framework to build upon for future development and implementation of behavioral norms and standards in cyberspace. The United Nation's Third Committee of the General Assembly and Economic and Social Council focuses on the criminal and economic exploitation of cyberspace, recognizing the necessity for cooperation between states and commercial industry to establish and adopt standards of behavior to combat cybercrime and close the loopholes between state cyber borders.[87] Furthermore, beginning in 2004, the United Nations formed the Group of Governmental Experts (GGE) to research and develop recommendations for standards of behavior in cyberspace. The organization does this by drawing best practices from practitioners and technical experts because there is a general acceptance of the concept and idea.[88] Through existing suborganizations and resolutions, the United Nations is able to consolidate best practices and innovative recommendations in order to present an acceptable collection of cyberspace behavioral norms and standards.[89]

Additionally, the United Nations formed both the Working Group on Internet Governance and the International Telecommunications Union (ITU) for the purpose of

---

[86] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 15.

[87] Ibid., 35-36.

[88] George R. Lucas, Jr., "Emerging Norms for Cyberwarfare," 21.

[89] Larry Clinton, "A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense," *Journal of Strategic Security*, 4, no. 2 (June 2011): 106, accessed September 25, 2017, https://doi.org/10.5038/1944-0472.4.2.6.

determining whether public or private authorities should govern cyberspace and "build confidence and security in the use of information and communications technology."[90] Specifically, the ITU has focused on improving legislative standards, creating international organizations designed to promote cooperation and information sharing to prevent future cyberattacks, and proposing standards for states to protect their critical infrastructure.[91]

Over time, the work of the committees and suborganizations realized increased levels of cooperation as members shifted their focus from individual national interests to the shared international interests in the cyber domain: cybercrime, capacity, and security. [92] Additionally, the use of established United Nations committees leveraged the member states' ability to gather experts, increase diversity of opinion, and advocate desired outcomes to a larger, global audience of decision makers.

Building on the work of the committees and suborganizations, the United Nations uses established administrative processes to facilitate the generation and approval of behavioral norms in cyberspace. The alliance understands and appreciates the importance of the commercial industries in the cyber domain. Resolutions proposed by the Economic and Social Council and Second Committee of the General Assembly specifically invite and advocate for commercial sector inclusion within ongoing and future dialogues regarding cyberspace standards and security. Additionally, United Nations General Assembly Resolutions 58-199 and 64/211 require United Nations organizations to seek to include commercial sector representatives in committees, conferences, and other venues set to discuss cyberspace security.[93] Using the processes and

---

[90] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 3-4; Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 29.

[91] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security," 29-30.

[92] Ibid., 18-19.

[93] Ibid., 38, 40, 44, 61-64.

inclusivity mandate as a baseline for resolution development and presentation, the alliance ensures political control, inclusivity, and institutional authority. Recently in 2010, the United States joined the Russian Federation and fourteen other states in the United Nations Cyber Arms Control Collaboration. The goal of the coalition is to prevent a cyber arms race and provide a foundation for future United Nations efforts at behavioral norms development.[94] In 2011 and 2015, China and the Russian Federation proposed a code of conduct for cyberspace to the General Assembly. Finally, in 2015, the United Nation's GGE submitted its third report, including its own proposal for standards of behavior in the cyber domain.[95]

The momentum is growing and states around the globe continue to offer recommendations for a stable and secure cyber domain. By satisfying the criteria recommended to successfully draft and adopt standards, the United Nations is poised to handle the task of developing, for international approval, acceptable responses to cyberattacks that will go a long way towards increasing stability and trust between states operating in cyberspace.

Conclusion

In many cases, established laws or instructions provide the necessary guidance to inform states how to behave or interpret ongoing actions within their sovereign territory and areas of influence. Cyberspace is a universal domain unconstrained by any one state, yet it connects each country to one another in ways both virtual and physical. Further, it is seen as essential to the progress of modern governments and businesses. Because cyberspace lacks a well-defined physical location and clear geographic boundaries, governments must pursue new or nontraditional ways of conducting business on the internet and developing standards of behavior.[96]

---

[94] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 23-24.

[95] Emilio Iasiello, "What Happens if Cyber Norms are Agreed To?" 31.

[96] George R. Lucas, Jr., "Emerging Norms for Cyberwarfare," 15.

Cyberspace has a nature that causes security risks for the international community and states. These risks, when ungoverned and allowed to grow, have specific effects that negatively influence relationships among states. Over time, the adverse impacts of a lack of behavioral norms lead to a potential for conflict escalation between states due to misperception of a state or non-state actor's intent.[97] The international community should develop and adopt behavioral standards and norms that provide acceptable responses to cyberattacks. The international acceptance of the norms adds legitimacy to cyberattack responses and ensures the norms address the concerns of a timely action, an appropriate level of response that avoids unintentional escalation, and preserves any perceived, if fleeting, asymmetric advantage in cyberspace.

One method to accomplish this task and moderate a state's reaction to a cyberattack is to develop and use a common lens to interpret and respond to an actor's actions. Standards of behavior among actors in cyberspace serve as a practical lens or common language that states can use to understand the intent behind an actor's cyber operations. Further, behavioral norms and standards provide stability among states by managing expectations and consequences and strengthening trust and relationships.

The preferred venue to produce and adopt standards of behavior in cyberspace is an alliance that has an existing apparatus that emphasizes political control, is inclusive of the many stakeholders with interest in cyberspace, and has the capability to enforce the agreed-upon standards.[98] Additionally, the alliance used to develop the standards and norms should mirror cyberspace's global scale and interconnectedness among actors because it adds relevance to the document and increases the likelihood of universal application.[99]

---

[97] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 31.

[98] Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," 3.

[99] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," 460.

Bilateral and multilateral, regional alliances have made great strides towards securing their cyber vulnerabilities and establishing behavioral norms required between alliance members and those states who desire to conduct business within their territory. Unfortunately, these successes have been unable to influence the global community because the alliances are territorially limited. It is necessary, therefore, to utilize a multilateral, global alliance able to leverage existing administrative processes to present and approve agreements to a membership. The United Nations is a multilateral, global alliance that meets these criteria and successfully generates and approves international standards of behavior in cyberspace.

Those opposed to multilateral, global alliances taking the lead in the development and implementation of international behavioral norms cite three reasons for this belief. First, the United Nations has 193 member nations unwilling to compromise their national interests and support a common goal of stability in cyberspace. Second, the commercial sectors should lead any development and implementation of international standards of behavior in cyberspace because they have more experience in the domain and exert greater authority over the cyberspace infrastructure.[100] Finally, an alliance of this size lacks the authority to unequivocally bind and enforce application of an agreed-upon set of standards.[101] However, it is the ability of the United Nations to reach compromise through decision makers vested with the political authority to add strength to discussions, its inclusive dialogue with all stakeholders in cyberspace, and the United Nations Charter that binds member nations to abide by the decisions of the alliance that make the United Nations a preferred choice to improve stability between states in cyberspace. The United Nations' inherent advantages of existing administrative protocols, binding membership regulations, and a core imperative to promote security and peace between states based on all national interests rather than the interests of an individual state further strengthen the position that

---

[100] Paul Cornish, David Livingstone, Dave Clemente, and Claire Yorke, *On Cyber Warfare*, 26.

[101] Joe Burton, "NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation," 340.

the United Nations is capable of achieving success. It is these traits of the United Nations that support it as the preferred venue to develop and adopt behavioral norms in cyberspace.

Bibliography

Bendiek, Annegret. “Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection.” *Transatlantic Academy Paper Series*, no. 1 (2014). Accessed September 26, 2017. http://www.transatlanticacademy.org/sites/default/files/publications/Bendiek_TestsofPartnership_Feb14_web.pdf.

Boeke, Sergei, Caitríona H. Heinl, and Matthijs A. Veenendaal. “Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe.” *Cyber Conflict (CyCon): 2015 7th International Conference on Architectures in Cyberspace* (Summer 2015): 69-80. Accessed September 28, 2017. http://ieeexplore.ieee.org/abstract/document/7158469/.

Burton, Joe. “NATO’s Cyber Defence: Strategic Challenges and Institutional Adaptation.” *Defence Studies* 15, no. 4 (December 2015): 297-319. Accessed September 26, 2017. https://doi.org/ 10.1080/14702436.2015.1108108.

Clinton, Larry. “A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense.” *Journal of Strategic Security* 4, no. 2 (June 2011): 97-112. Accessed September 25, 2017. https://doi.org/10.5038/1944-0472.4.2.6.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. *On Cyber Warfare*. The Royal Institute of International Affairs Report. London: Chatham House, 2010. Accessed September 26, 2017. https://pdfs.semanticscholar.org/194c/24d15590a0cc6b39658db996eba85600cff8.pdf.

Deibert, Ronald J., and Masashi Crete-Nishihata. “Global Governance and the Spread of Cyberspace Controls.” *Global Governance; Boulder* 18, no. 3 (September 2012): 339-61. Accessed October 2, 2017. https://search.proquest.com/docview/1034977196/abstract/AF19564F3E9C4595PQ/1.

Federal Department of Foreign Affairs. “Participating States of the Montreux Document.” *The Federal Council, the Portal of the Swiss Government*. Last modified November 11, 2017. Accessed February 10, 2018. https://www.eda.admin.ch/eda/en/home/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/participating-states.html.

Finnemore, Martha, and Duncan B. Hollis. “Constructing Norms for Global Cybersecurity.” *The American Journal of International Law*; Washington 110, no. 3 (July 2016): 425-79. Accessed November 3, 2017. https://search.proquest.com/docview/1830058161/abstract/4612A6ADBDB44F13PQ/1.

Finnemore, Martha, and Kathryn Sikkink. “International Norm Dynamics and Political Change.” *International Organization; Cambridge* 52, no. 4 (Autumn 1998): 887-917. Accessed November 1, 2017. https://search-proquest-com.lumen.cgsccarl.com/docview/219221738?pq-origsite=summon.

Garside, Debbie. “Cybersecurity Trends for 2018.” *Chief Security Officer (CSO) Online*. Last modified December 8, 2017. Accessed January 14, 2018. https://www.csoonline.com/article/3241122/cyber-attacks-espionage/cybersecurity-trends-for-2018.html.

Grisham, Lori. “Timeline: North Korea and the Sony Pictures Hack.” *USA Today*. Last modified January 5, 2015. Accessed March 25, 2018. https://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

Hill, Richard. “Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT.” *Cyber Conflict (CyCon): 2015 7th International Conference on Architectures in Cyberspace* (Summer 2015): 119-34. Accessed September 28, 2017. http://ieeexplore.ieee.org/abstract/document/7158473/.

Iasiello, Emilio. “What Happens if Cyber Norms are Agreed To?” *Georgetown Journal of International Affairs; Washington* 17, no. 3 (Fall 2016): 30–37. Accessed October 1, 2017. https://search.proquest.com/docview/1924880335/abstract/A910C9778B9840C2PQ/1.

Internet Live Stats. “Internet Users.” *Internet Live Stats*. Last modified July 1, 2016. Accessed December 12, 2017. http://www.internetlivestats.com/internet-users/.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York, NY: Simon & Schuster, 2016.

Ladnier, Patricia. “Critical Infrastructure Protection and Federal Statutory Authority for the Departments of Homeland Security and Defense to Perform Two Key Tasks.” Monograph, US Army Command and General Staff College, 2017.

Lucas, George R., Jr. “Emerging Norms for Cyberwarfare.” In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser, 13-33. New York: Oxford University Press, 2016.

Maurer, Tim. “Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security.” *Science, Technology, and Public Policy Program: Explorations in Cyber International Relations Project* (2011). Accessed November 26, 2017. https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf.

Maybaum, Markus, and Jens Tölle. “Arms Control in Cyberspace-Architecture for a Trust-Based Implementation Framework Based on Conventional Arms Control Methods.” *Cyber Conflict (CyCon): 2016 8th International Conference on Cyber Power* (Summer 2016): 159-73. Accessed September 28, 2017. http://ieeexplore.ieee.org/abstract/document/7529433/.

Mendoza, Joshua A. “Cyber Attacks and the Legal Justification for Armed Response.” Monograph, US Army Command and General Staff College, 2017.

Mikolic-Torreira, Igor. *A Framework for Exploring Cybersecurity Policy Options*. Research Report, RR-1700-WFHF. Santa Monica, CA: RAND, 2016.

Nakashima, Ellen. “Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies.” *The Washington Post*. Last modified March 19, 2010. Accessed December 29, 2017. http://www.washingtonpost.com/ wp-dyn/content/article/2010/03/18/ AR2010031805464.html.

Orji, Uchenna Jerome. “Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?” *Cyber Conflict (CyCon): 2015 7th International Conference on Architectures in Cyberspace* (Summer 2015): 105-18. Accessed September 28, 2017. http://ieeexplore.ieee.org/abstract/document/7158472/.

Robinson, Neil. “NATO: Changing Gear on Cyber Defence.” *NATO Review Magazine*. Last modified 2016. Accessed January 14, 2018. http://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/EN/index.htm.

Schmitt, Michael N., and Liis Vihul. "The Nature of International Law Cyber Norms." *Special expanded issue, The Tallinn Papers*, no. 5 (2014). Accessed October 2, 2017. http://www.ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%205%20Schmitt%20and%20Vihul.pdf.

Simon, Sheldon W. "Conflict and Diplomacy in the South China Sea." *Asian Survey; Berkeley* 52, no. 6 (December 2012): 995-1018. Accessed February 1, 2018. http://dx.doi.org.lumen.cgsccarl.com/10.1525/as.2012.52.6.995.

Thatcher, Margaret. *The Downing Street Years*. 1st ed. New York: HarperCollins, 1993.

Tirpak, John A. "Leaked NPR Draft Misinterpreted on Nuclear Response to Cyber, Selva Says." *Air Force Magazine*. Last modified January 31, 2018. Accessed February 1, 2018. http://www.airforcemag.com/Features/Pages/2018/January%202018/Leaked-NPR-Draft-Misinterpreted-on-Nuclear-Response-to-Cyber-Selva-Says-.aspx.

United Nations. Chapter IV: The General Assembly Functions and Powers. June 26, 1945. Charter of the United Nations. Accessed December 27, 2017. http://www.un.org/en/sections/un-charter/chapter-iv/index.html.

United Nations. Chapter V: The Security Council Functions and Powers. Charter of the United Nations. June 26, 1945. Accessed December 27, 2017. http://www.un.org/en/sections/un-charter/chapter-v/index.html.

US Department of Defense, Joint Staff. Joint Publication (JP) 3-12(R), Cyberspace Operations. Washington, DC: Government Printing Office, 2013.

US Department of Defense. "The Department of Defense (DoD) Cyber Strategy." Washington, DC: Government Printing Office, 2016. Accessed August 21, 2017. https://www.defense.gov/ Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_ for_web.pdf.

US President. Executive Office of the President. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." February 2003. Accessed February 9, 2018. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.