Conflict in Cyberspace: How International Legal Norms Can Reduce Military Escalation in Cyberspace

By Nikolas Ott

Abstract

This paper examines the current technical and legal considerations around the development of international legal norms and confidence-building measures in cyberspace. With an emphasis on state-based armed attacks and the use of force in cyberspace, it summarizes the current status of international efforts within the United Nations and several regional organizations. The paper concludes with several suggestions on how policymakers can reduce the gap between technological and legal considerations.

THE CURRENT DISCUSSION

Cyberspace is an increasingly important operational environment for surveillance, espionage, military conflict, and beyond. Offensive military operations in cyberspace especially pose a new challenge for the applicability and enforcement of public international law. Since 2013 the United Nations has acknowledged that conflict in cyberspace is a serious concern for the international community.[1] States agree that cooperation is essential to reduce risk and enhance security within cyberspace.[2] Given this commitment, it is fair to say that states believe that further escalation in cyberspace can be prevented through the implementation of international regimes[3], treaties[4], or agreements[5]. However, when it comes to military activities, few states are currently willing or able to engage in comprehensive negotiations on treaties governing military use of cyberspace.[6]

Below the threshold of international treaties, there are norms, which have the potential to be codified or implemented through practice. The same applies to confidence-building measures (CBMs) as means to further promote this dialogue. Many international institutions are facilitating such talks at this stage.[7] However, most of these talks are focused on law enforcement cooperation against organized cyber-crime rather than military activities in cyberspace.[8]

During the latest round of consultations of the United Nations Group of Governmental Experts on Cybersecurity (UN GGE), the group hardly addressed military activities as relevant to their discussion of norms and principles in cyberspace. Instead, in their July 2015 report to the UN General Assembly, the relevant section focused on critical infrastructure and Information and Communications Technology (ICTs).[9]

While the UN GGE reports from 2013 and 2015 demonstrate that there is a general agreement that existing international laws — such as the laws of armed conflict — do indeed apply to cyberspace, the actual scope of their application remains contested.[10] Some analysts argue that the latest UN GGE report made some important steps in clarifying the applicability of

the laws of armed conflict in cyberspace.[11] Even so, the discussion of a definition of armed attack and the use of force in cyberspace is hardly over.[12]

A dialogue on legal norms is crucial to harmonizing different interpretations among countries, and there are several key developments that try to clarify the scope and extent to which existing international law applies to cyberspace.[13] However, the current discourse on norms, at least at the UN level, seems to be stagnant.[14] With this stalemate in mind, this essay will examine under what conditions international legal norms and CBMs contribute to the reduction of military escalation within cyberspace and how this development can be facilitated. Given the scope of this paper, the analysis will be limited to the discussion of legal norms surrounding an armed attack and the use of force in cyberspace.

First, this essay will outline several important characteristics of cyberspace that are relevant for any potential methods of implementing international legal norms and CBMs. Second, it will discuss technical considerations with regard to offensive and defensive military activity in cyberspace. Third, it will review the current policy debates surrounding the use of force and armed attacks in cyberspace. Fourth, it will outline present efforts to reduce conflict in cyberspace with a focus on international legal norms and CBMs. Lastly, it will draw conclusions from the technical and policy perspectives and propose potential next steps to bridge the gap between the two.

IMPORTANT CHARACTERISTICS OF CYBERSPACE

While some scholars argue that existing frameworks for analyzing the use of force and armed attacks can be applied to cyberspace as well,[15] military action in cyberspace has several unique features that are important to understand when aiming to establish functioning legal norms.

Attribution in cyberspace remains a core challenge. Given the wide variety of options for acting anonymously in cyberspace, guaranteed attribution of every single attack remains technically impossible.[16] The most sophisticated intelligence agencies might be able to identify the computer that was used to create a certain code or to carry out an attack, but this does not mean that they know who was actually using the computer or whether the computer was a means to carry out the attack, while the attack was actually planned somewhere else. In many situations hijacked computers around the world are used to further complicate tracing an attack back to its originator. While some experts argue that attribution in cyberspace is no longer a challenge, it remains unclear about what kind of attribution they are actually referring.[17]
Most security experts remain reluctant to say attribution, especially for international legal purposes, has been solved. Given the ongoing evolution of technological capabilities, experts in most cases are able to track a connection to a machine. However, as noted above, connecting this computer to the user is extremely difficult. This problem is oftentimes referred to as the "endpoint security issue,"[18] effectively tying the device to the person is currently almost impossible.

The number of potential actors is significantly higher compared to other domains since the technical threshold for entering cyberspace for offensive purposes is relatively low.[19] The confusion surrounding the origin of the Sony hack reflects this trend. Even weeks after the incidents, security experts were not absolutely sure who was behind the attack.[20] The reason for this was the simplicity and lack of sophistication of the hack. In fact, the attack could have been created easily many by non-state actors. Ultimately, a deep review of the *intent* of the attackers, combined with additional intelligence was necessary to be able to determine with reasonable confidence that North Korea was behind the attack.[21]

If a few individuals with experience in hacking might be able to conduct operations similar to a highly sophisticated military of an industrialized country,[22] then this leads to an erosion of (hard) power that we have not seen in recent decades. The low cost of initiating unsophisticated offensive operations in cyberspace also means that it is easier for unconventional players, oftentimes non-state actors, to enter the stage and further complicate inter-state discussions and negotiations to introduce mechanisms that could reduce conflict in cyberspace. However, experts believe that ordinary hackers are not able to create computer worms like Stuxnet, the advanced malware deployed in an attempt to sabotage Iran's nuclear facilities.[23] Such sophisticated attacks are generally labeled as "Advanced Persistent Threats" (APT) given the significant amount of human intelligence and information that is required to deploy them.[24] These attacks require the attacker not only to create a malicious virus and hack into a network, but also require an intimate knowledge of software bugs, network vulnerabilities, human intelligence, and on-the-ground operations.[25]

Given the borderless design of cyberspace, the geographical location of an attacker and its target no longer play a major role. Distance used to be an impediment for confrontation. Moreover, one could build walls, fences, or use natural borders such as mountains or water to create distance. In cyberspace, such borders do not exist by design and it is difficult at this stage to artificially create them. In fact, the entire concept of distance becomes obsolete in cyberspace. Once an attacker has access to the victim's network or computer, data extraction, surveillance or even destruction may occur almost instantaneously. It is yet to be seen how this trend will shape future geopolitical strategic thinking. Lastly, incorrect identification of the origin of an attack, commonly referred to as false flag events, is more likely to occur in cyberspace than in traditional military domains.

TECHNICAL CONSIDERATIONS ON LEGAL DEFINITIONS OF OFFENSIVE ACTIVITY

Based on the previously outlined characteristics of cyberspace, it comes as no surprise technical considerations play an important role in developing and implementing functional norms. It is important to acknowledge there are no absolutes in cybersecurity. There is no absolute security, no absolute attribution, no absolute detection, etc.

When one observes internet traffic, it is impossible to know immediately what a certain package of data may contain. The design of the package itself is neutral. Recent technological advancements such as deep package inspection make it easier to detect known malign internet

traffic, but they cannot stop new kinds of attacks. Ultimately, intent is what distinguishes Google's testing of its own networks for vulnerabilities from outside hackers who are stealing from that same network. While Google's employees most likely have good intentions when improving their network defense capabilities, the hacker's intentions could be characterized as malign. Thus, the intent of an action is crucial to determining whether the action is offensive or defensive.

In the case of the United States, legal definitions also have an effect on the cyber-attack threshold analysis. While computer network exploitation (CNE) and computer network attacks (CNA) are technically the same,[26] they are treated differently from a legal perspective.[27] A perceived CNA might cause a significantly different response from a perceived CNE, though the technical symptoms of both activities look identical. From a technological perspective, there is no such thing as "passive hacking."[28] Making such a determination requires knowledge of the actor's intent.

This technical consideration creates huge challenges for the development of legal norms because almost every activity related to cybersecurity could be identified as a potential "dual use" good, depending on the intention of the actor. Moreover, cyber defense experts might not be able to distinguish immediately whether a network intrusion is done to spy on, steal, or destroy data or infrastructure. Any legal norm aimed at reducing conflict in cyberspace will have to acknowledge this reality. The U.S. Department of Commerce's Bureau of Industry and Security's latest legal effort to introduce international regulations on this issue failed due to the ambiguity in the proposed legal language.[29]

THE USE OF FORCE AND AN ARMED ATTACK IN CYBERSPACE

Scholars and experts continue to discuss what kinds of actions are necessary to constitute a conflict in cyberspace. In fact, there is no universally accepted definition of cyber warfare. Authors such as John Arquilla, Thomas Rid, Peter Singer, and many others have searched for a consensus definition, but so far no definition has been widely endorsed among states.[30] The lowest common denominator seems to be that the definition simply depends on the circumstances, the involved actors, the target, the intent, and the scale of the event. So far, scholars argue that we have not yet seen long-term offensive cyber activities, but we have experienced several events in which cyber attacks supplemented kinetic attacks, such as in Georgia in 2008.[31]

Agreeing on a definition for cyber warfare is important because it helps reduce ambiguity and complexities; this evolution can facilitate the reduction of conflict in cyberspace. Using Thomas Rid's narrow interpretation[32] of cyber war referring to an active force compelling the enemy to your will plus a political goal or intention,[33] we are not yet living in an environment of cyber war. In fact, the 2015 Worldwide Threat Assessment of the U.S. Intelligence Community came to a similar conclusion. It stated that ". . . the likelihood of a catastrophic [cyber] attack from any particular actor is remote at this time. . . . We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security."[34]

But even before theorizing on the existence of cyber war, one needs to define what an "armed attack" and the "use of force" in cyberspace actually mean. Several states, international organizations, researchers, and other actors have come up with potential definitions.[35] While few states acknowledge this argument, most of them actually follow a very crude logic: an armed attack in cyberspace is when we say it was an armed attack.[36] Thus, depending on the actors' perspective, they will either observe or not observe "cyber war." Similar discussions take place around the definition of the "use of force" in cyberspace.[37]

Generally, the UN Charter, the Laws of Armed Conflict, and subsequent legal interpretations of these documents are considered as foundational legal documents for legal analysis of an armed attack and the use of force in cyberspace. Additionally, customary international law is considered a secondary source for the legal interpretation of state practice. Article 2(4) in the UN Charter prohibits the use of force except in situations of self-defense (Article 49) or through UN Security Council approval under a Chapter VII resolution. Lastly, Article 51 refers to the "inherent right of individual or collective self-defense if an armed attack occurs."[38] As mentioned above, the legal discussion about the correct application of these terms for cyberspace is still ongoing.[39] This leaves current politicians and policy-makers with a dilemma: How do you act in a situation in which precise legal definitions have not been generally agreed upon?

CURRENT INTERNATIONAL EFFORTS TO REDUCE CONFLICT IN CYBERSPACE

Based on the existing international legal framework, the further development of international legal norms requires a multilateral negotiation and development process. CBMs and capacity building can also be implemented on a regional level. Currently, the discussion on the scope of existing legal frameworks largely takes places within the UN GEE and regional organizations. Parallel to that analysis, a discussion on the development of new legal norms for cyberspace, such as the potential international code of conduct for information security, is also taking place within the UN.[40] CBMs and capacity building are mostly taking place within regional organizations, such as the Organization for Security Cooperation in Europe (OSCE), the Organization for American States (OAS), and the Association of Southeast Asian Nations (ASEAN). The European Union (EU) is also actively engaged in providing capacity building for its member states and its own institutions.

In 2013 the UN GGE published for the first time a consensus report in which it identified three ways to reduce conflict in cyberspace: legal norms, CBMs, and capacity building.[41] While this list contains an implicit hierarchy, all three methods are crucial to improving the effectiveness of any one of them. In fact, as this paper will argue, all three are reinforcing and supporting each other. Since that report, the UN GEE has been trying to identify ways to deal with cybersecurity challenges on an international level. In July 2015, the UN GEE released its latest report proposing additional norms of responsible state behavior and the standing of international law in cyberspace.[42] However, the new norms and principles of the 2015 report focus on ICTs and nation-states' critical infrastructure.

Sadly, the latest UN GEE report "did not reconcile the ongoing tensions over the scope of state sovereignty with respect to the Internet."[43] This challenge remains a core issue that cannot be addressed without extensive and constructive contributions from a variety of nation-states and non-state actors. This growing frustration on the limited power of the UN GEE, which is technically a UN working group that relies on an annual renewal of its mandate, is oftentimes reflected in calls for the establishment of a body with more authority. [44] However, it seems unlikely that key actors such as the United States, China, and Russia have a particular interest in giving away authority to influence the international agenda on cybersecurity.

Beyond the UN GGE, a variety of actors and institutions have initiated several projects in order to harmonize the different perspectives on military activities in cyberspace. The following pages will provide an overview of these efforts and draw conclusions on the necessary next steps to help codify legal norms for cyberspace, while keeping in mind the technological circumstances within which these legal norms must operate.

Dispute around Legal Norms Governing Use of Force

Norms help enter a new area of activity where existing laws are inapplicable or non-existent. They help pave the way through non-binding principles. Even if they do not give rise to a new law, norms create expectations and foster discussion among actors. In fact, norms shape expectations, which are critical for states to rationally calculate their interests and define behavior. Shared expectations through norms help avoid the cost of conflict, because they reduce friction and create greater predictability, which reduces transaction costs. However, there is no clear-cut hierarchy among the many norms that govern cyber activities; this confusion is why scholars like Joseph Nye refer to this environment as a regime complex.[45]

When it comes to states' efforts to reduce conflict in cyberspace, international legal norms have received considerable attention in recent years. This is particularly true for states that believe in the value and relevance of the current international legal order (ILO). In fact, the international community largely agrees that existing international law applies in cyberspace. However, "the guidelines on how this should be done in practice are only beginning to emerge."[46] Several key state actors, such as China and Russia, disagree with the Western approach to the ILO and are making efforts to adjust it according to their preferences.[47] Their efforts to implement an international code of conduct for information security are the most prominent, but not the only example of such efforts. [48]

Under current circumstances, "cybersecurity" and "information security" are the two main themes that are discussed and debated among states. For the United States, cybersecurity largely relates to the "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[49]

In contrast, China defines information security as an issue that "involves not only the risks arising from the weakness and interconnected nature of the basic information infrastructure, but also the political, economic, military, social, cultural, and numerous other types of problems

created by the misuse of information technology. Both of these factors are worthy of concern when studying the issue of information security."[50] Comparing these two, one notices that while some portions of both themes have overlap, there is considerable disagreement about the very idea of security, let alone about potential definitions of an armed attack and the use of force in cyberspace.

Third parties such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCoE) are also contributing to this discussion. However, the CCDCoE's Tallinn Manual on the International Law Applicable to Cyber Warfare largely reflects ideas and perceptions of academics from NATO membership countries.[51] Moreover, the Tallinn Manual's definition and scope is also contested and not accepted by many non-NATO member countries.

Beyond the political disagreements among states, the technical constraints outlined above further complicate the development of effective legal norms. This implication leads to the question of whether the current emphasis on international legal norms is in fact helpful to solve the challenge of conflict in cyberspace. Do international legal norms help prevent, or at least reduce conflict in cyberspace? There is a wide spectrum[52] of scholarly work on this topic and the key conclusion that can be drawn is that international cooperation is understood to be "essential to reduce risk and enhance security," just as the UN GGE Report stated already in 2013.[53] But it remains disputed what kind of cooperation is necessary, which actors will be involved, and how this cooperation can be institutionalized.

The Role of Confidence-Building Measures to Reduce Conflict in Cyberspace

Given the highly political circumstances under which international legal norms are discussed, CBMs are considered to be a good alternative to identify areas of cooperation and reduce mistrust among nation-states. In fact, CBMs between states are generally considered to be "one of the key mechanisms in the international community toolbox aimed at preventing or reducing the risk of a conflict by eliminating the causes of mistrust and miscalculation between states."[54]

Norms reflect *values*, which are ideas that exist among actors and therefore aim at a certain end state or a goal. On the other hand, CBMs are considered to be *means* because they provide the process of getting to the end state that norms envision.[55]

Establishing CBMs in cyberspace shares some of the challenges that face the effort to develop norms, including state sovereignty, the non-physical nature of cyberspace, and the significant number of non-state actors. The lack of reasonable attribution in cyberspace makes it difficult to implement CBMs that are based on verification, a common feature among traditional CBMs. These challenges need to be acknowledged by all involved actors before innovative CBMs for cyberspace can be developed.

Once acknowledged, CBMs have several features that cannot be accessed through pure discussions around norms. CBMs help prevent miscalculation, misunderstanding, and escalation between states. They do not require reaching consensus on everything. It is possible to work around the edges of contested issues and gradually move to a more comprehensive agreement.

Generally, there are four types of CBMs that are relevant in cyberspace: collaborative, crisis management, restraining activities, and increasing engagement.

CBMs on collaboration are designed to share information, provide transparency, and build trust. They provide a platform for dealing with the unique challenges of cyberspace. They foster trust by creating channels for communication. Collaborative CBMs also contribute to transparency, accountability, and stability. The OSCE is one of the first international organizations that implemented a first round of collaborative CBMs aimed at information sharing and regular meetings. Proposals for additional CBMs on collaboration include the establishment of a framework for joint investigations, the application of environmental law in cyberspace, and increased compliance policing through best current practices.

CBMs on crisis management are intended to manage tense moments to avoid outbreak of major wars between nation-states. In cyberspace, such efforts would require the inclusion of non-state actors as observers or policing forces. Current practical proposals on crisis management CBMs include the functional alignment of crisis emergency response teams (CERTs) to increase transparency. Actors that share the CERTs with other governments before a crisis hits know immediately whom to reach out to in a tense situation. To further promote stability, some suggest the implementation of a multilateral cyber "hotline," which should also include private and social sector actors to keep them informed about ongoing developments. Lastly, scholars recommend fostering accountability in cyberspace through the establishment of a cyber adjudication and attribution council. Such an international body should be able to investigate and assign responsibility for cyber crises that could spiral into conflict. It could also serve as local arbitration court to avoid conflict. However, the challenges surrounding attribution in the cyber domain loom over the implementation of such a council.

CBMs aimed at increasing engagement with non-state actors are also crucial in cyberspace. Stronger engagement across both sides would create leverage for international technical regimes and help develop norms. This could be done by facilitating existing regimes, such as the Internet Engineering Task Force, Internet Corporation for Assigned Names and Numbers, or the World Wide Web Consortium to work with governments to set norms. Moreover, neutral activists' entanglement and support could be fostered. This would encourage and support security researchers to collaborate across borders and thus increase the discussion and engagement of technical, scientific, and legal experts across the world.

CBMs aimed at restraining activities could help on three levels: increasing stability of the internet backbones and infrastructure by creating target restrictions and neutrality; improving accountability by asking states to declare responsibility for behavior within their territory; and enhancing transparency by joint research on the applicability of international human rights law in cyberspace.

CBMs are not designed to substitute discussions around international legal norms. In fact, the feasibility of CBMs depends on the *parallel* development of international legal norms. Instead of looking at CBMs as a replacement of legal norms, both should rather be considered as reinforcing methods that help reduce conflict in cyberspace. Eventually, both paths may lead to the codification of best practices, behavior, and norms within cyberspace.

Ultimately, the main challenge that all of these proposals face is identifying clear and precise language that reflects the complexity of the technical circumstances while still being understandable by policymakers. The OSCE successfully bridged this gap in its first set of CBMs, but it remains the only international body that has made this effort.[56] Closing this bridge between technology experts, policymakers and lawyers should be at the core of any future CMB process.

TAKING STOCK AND MOVING FORWARD: BRIDGING THE GAP BETWEEN TECHNOLOGY AND LEGAL NORMS

When considering technological considerations with the legal and political challenges, one quickly notices that the two worlds operate according to very different principles and conditions. Politics and law develop much more slowly than technology. While technological development is driven by the adoption of new features by users, politics is driven by long negotiations and concludes in compromise or agreement. In the case of cyberspace, the technological constraints are significant and pose serious challenges to policy-makers and lawyers. Worse still, in light of recent discussions about separating different parts of the Internet, introducing backdoor access to encryption standards, and forcing companies to store data within certain jurisdictions before being allowed to operate, the gap between what technologists can do and what policy makers think technologists can do seems to be growing. The most relevant example for this paper is the argument from lawyers to establish a framework that distinguishes offensive from defensive cyber operations.[57]

Unfortunately, lawyers dominate the current discussion around legal norms in cyberspace. Only a few technology experts, such as Bruce Schneier, a fellow at the Berkman Center for Internet and Society at Harvard Law School, are engaged in discussions around norms. However, any discussion about legal norms in cyberspace is dependent on the technological environment in which those norms are supposed to be implemented. One good example to highlight this challenge is attribution in cyberspace. Norms in cyberspace only work if the actors believe that they can be accused of doing something wrong which requires attribution. Norms in a world without attribution are much harder to enforce because we tend to enforce norms by assigning responsibility.

Instead, many analysts look at the victims of attacks and draw conclusions about potential attackers through intuitive and non-empirical reasoning. However, given how easy it is to create false flags within cyberspace, this approach has significant limitations. Instead, the most powerful intelligence agencies, such as the NSA, are using a multitude of lawyers to assign attribution. However, such methods do not help create mechanisms for developing legal norms at the international level.

The same problem occurs with efforts to distinguish cyber espionage for intelligence purposes from cyber attacks. The two might look identical to an observer, so conveying intent can make the key difference in determining whether something is an offensive move or an intelligence operation.

These problems are crucial for understanding why it is so difficult to establish trust and confidence within the military sphere of cyberspace. Inspecting each other's military infrastructure, as was common for nuclear facilities during the Cold War, is basically useless because the *intent*, and not the technological *design*, of a cyber operation determines whether it is offensive or defensive. This key difference is not yet widely understood. So how do we move forward from here?

While states have managed to bring engineers and lawyers together in the past, the difference here is that states have not yet identified ways to deal with the truly global design of cyberspace.[58] This has led to a clash of digitalization with pre-existing norms, structures, and laws. Acknowledging this problem is an important step in the right direction. In order to close the gap between technology experts and lawyers, some of the following steps could be initiated.

First, existing international platforms such as the UN GGE need to receive a stronger mandate that is not limited to a yearly renewal through the UN General assembly. The negotiations have reached a level of complexity where internal capacity building, especially on the technological side, is crucial for further discussion. Simultaneously, such a reform should also provide nations with an increasingly large portion of cyberspace users — such as India, Brazil, and China — with more room to express their political, legal, and technological concerns through diplomatic channels.

Second, by providing the government experts with a more sustainable framework, it will also be easier to include non-state actors in the discussion. While the current framework gives some room for their voices, they are not well integrated into discussions. By opening the door to internet businesses (such as internet service providers), technology experts, and other non-state actors, future policy decisions are more likely to be technologically feasible to implement.

Third, once states accept that the inclusion of non-state actors helps reduce conflict potential and increase trust internationally, this process must be accompanied by the establishment of a database with relevant legal and technical terms. A prominent example of this idea is the New America Foundation Global Cyber Definitions Database,[59] which was supported by the OSCE. Such efforts will increase understanding of different points of view across sectorial and jurisdictional borders. Databases should also help reduce complexity from both the legal and technical sides.

Fourth, a significant increase in capacity building among current diplomats and policymakers would help them understand the technological characteristics of cyberspace. The same holds true for information technology experts who lack a legal or policy background. Additionally, by bringing more technical experts from around the world together, a shared understanding of technical terms and knowledge can develop across countries. Such efforts exist within some countries and regions, but need additional support.

Fifth, the issue of how to avoid the disintegration of cyberspace needs more attention. The economic opportunities that a global cyberspace offers cannot be maintained in a segregated cyberspace. By raising awareness of the strong nexus between economic prosperity and

cyberspace, future negotiations will generate more responsibility, hopefully furthering an even better understanding of global cyberspace. Increased awareness and contact will also promote interdependence among states in terms of managing the infrastructure and maintenance of cyberspace.

Sixth, by acknowledging the importance of this issue, not just for today but for many generations to come, it is easy to understand why efforts to train future generations of policymakers, lawyers, and technology experts about the interdisciplinary challenges of governing conflict in cyberspace are crucial. Oxford University's Center for Doctoral Training in Cyber Security[60] and the Scholarship for Service Partnership for Interdisciplinary Research and Education program at New York University Law School[61] are among the first institutional programs of their kind. Hopefully we will see many more in the future.

All of the aforementioned steps would improve the conditions under which international legal norms and CBMs can contribute to the reduction of military escalation within cyberspace. It is now a matter of political will to implement these suggestions and maintain such commitments.

CONCLUSION

We have reason to worry about military confrontation in cyberspace. Be it in a full-scale cyberwar, or as component of a larger military activity, it seems reasonable to say that the militarization of cyberspace is on the rise. Fortunately, fora like the UN GGE, the OSCE, ASEAN, OAS, the EU, and many others are actively working on reducing conflict and setting limits for military engagement in cyberspace. However, many of these efforts are slow, or have become stuck, given their limited mandate.

Simultaneously, technological developments will continue to outpace policy and legal discussions. It is therefore important for both sides to acknowledge that they are operating in very different environments. This does not mean that either side has to fundamentally change its modus operandi. Instead, the situation highlights the importance of increased exchange of perceptions, ideas, and trends. Given the borderless design of cyberspace, these exchanges should occur on an international level, facilitated, but not dominated, by states.

There are many possible efforts to bridge the gap between technology experts, lawyers, and policy-makers. Such efforts include expanding the mandate for the UN GGE, reducing the centrality of state governments in negotiating a framework of cyber norms, maintaining a shared database of cross-sectorial knowledge, and connecting the importance of cyberspace with the growth of global economies.

Together these measures would increase awareness of the political, legal, technological, and economic nexus in cyberspace, thus reshaping discussions of state-based military escalation using cyber capabilities. Ultimately, such efforts will foster negotiations on international legal norms and CBMs for reducing military escalation within cyberspace and create conditions in which future dialogue can be more effective, sophisticated and sustainable. Cyberspace has

become a fundamental and inextricable realm of governmental activity. Maintaining a stable cyberspace is therefore not simply an interest but a necessity.

8. BIBLIOGRAPHY

Arquilla, John. “Cyberwar Is Already Upon Us.” *Foreign Policy*. February 27, 2012.

ASEAN. “ARF Work Plan on Security of and in the Use of Information and Communications Technologies.” ASEAN, May 7, 2015.

Beach, Sophie. “China and Russia Support ‘Cyber Sovereignty.’” *China Digital Times*, May 11, 2015, online edition.

Cardozo, Nate, and Eva Galperin. “What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?,” May 28, 2015.

Chernenko, Yelena. “Global Cybersecurity: 6 Questions on the Key Issues as Seen from Moscow.” *Russia Beyond The Headlines*. August 19, 2015. http://rbth.com/international/2015/08/19/global_cybersecurity_6_questions_on_the_key_issues_as_seen_from_48615.html.

Clapper, James R. “Worldwide Threat Assessment of the US Intelligence Community.” Washington D.C.: Office of the Director of National Intelligence, February 26, 2015.

Deeks, Ashley. “Tallinn 2.0 and a Chinese View on the Tallinn Process.” *Lawfare Blog*, May 31, 2015. https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.

Department of Defense. “Department of Defense Dictionary of Military and Associated Terms.” Department of Defense, November 15, 2015.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. “W32.Stuxnet Dossier.” Symantec, n.d.

Geers, Kenneth, Darien Kindlund, Ned Moran, and Rob Rachwald. “World War C: Understanding Nation-State Motives behind Today’s Advanced Cyber Attacks.” Technical report, FireEye, 2014. http://ver007.com/tools/APTnotes/2013/fireeye-wwc-report.pdf.

Giles, Keir, and William Hagestad. “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English.” In *Cyber Conflict (CyCon), 2013 5th International Conference on*, 1–17. IEEE, 2013. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6568390.

Healey, Jason, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd. “Confidence-Building Measures in Cyberspace - A Multistakeholder Approach for Stability and Security.” Washington D.C.: Atlantic Council, 2014.

Hirschfeld Davis, Julie, and David Sanger E. “Obama and Xi Jinping of China Agree to Steps on Cybertheft.” *New York Times*. September 25, 2015, online edition. http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

Hurwitz, Roger. “The Play of States: Norms and Security in Cyberspace.” *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322–31. doi:10.1080/10803920.2014.969180.

Joint Chiefs of Staff. “Cyberspace Operations.” Joint Publication 3-12 (R). Washington D.C.: Department of Defense, February 5, 2013.

———. “Information Operations.” Joint Publication 3-13. Washington D.C.: Department of Defense, November 20, 2014.

Kanuck, Sean. “Sovereign Discourse on Cyber Conflict Under International Law.” *Tex. L. Rev.* 88 (2009): 1571. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr88&section=56.

Kennedy, David. “The International Symposium on the International Legal Order.” *Leiden Journal of International Law* 16, no. 4 (December 2003): 839–47. doi:10.1017/S0922156503001523.

Kenneth Geers, ed. *Cyber War in Perspective*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Libicki, Martin C. “Would Deterrence in Cyberspace Work Even with Attribution.” Georgetown Journal of International Affairs, April 22, 2015. http://journal.georgetown.edu/would-deterrence-in-cyberspace-work-even-with-attribution/.

Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39, no. 3 (January 2015): 7–47. doi:10.1162/ISEC_a_00189.

Marks, Joseph. “U.N. Body Agrees to U.S. Norms in Cyberspace.” *Politico*. July 9, 2015. http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900.

Maurer, Tim. “Cyber Norm Emergence at the United Nations.” *Cambridge, MA: Belfer Center for Science and International Affairs*, 2011. http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

Meyer, Paul. “Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace.” *ICT for Peace Foundation*, September 4, 2015. http://ict4peace.org/another-year-another-gge-the-slow-process-of-norm-building-for-cyberspace/.

———. “Seizing the Diplomatic Initiative to Control Cyber Conflict.” *The Washington Quarterly* 38, no. 2 (April 3, 2015): 47–61. doi:10.1080/0163660X.2015.1064709.

Mudrinich, Erik. “Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem.” *Air Force Law Review 68* 68 A.F. L. Rev. (2012).

NATO. *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2013.

Nye, Joseph S. “The Regime Complex for Managing Global Cyber Activities,” 2014. http://dash.harvard.edu/handle/1/12308565.

Nye Jr, Joseph S. “Nuclear Lessons for Cyber Security.” DTIC Document, 2011. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA553620.

Organization for Security and Co-operation in Europe Permanent Council. “Decision No. 1106 Initial Set Of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies.” 975th Plenary Meeting. Vienna, Austria: OSCE, December 3, 2013.

Pawlak, Patryk. “Cyber Diplomacy.” Briefing. Brussels, Belgium: European Parliament, October 2015.

Permanent Representative of the People's Republic of China. "Submission to the United Nations General Assembly Resolution A/62/98," 2008.

Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan. Formal letter to the UN Secretary General - A/66/359. "Proposal for an International Code of Conduct for Information Security." Formal letter to the UN Secretary General - A/66/359, September 14, 2011.

Peterson, Andrea. "The Government Is Headed back to the Drawing Board over Controversial Cybersecurity Export Rules." *Washington Post*. July 29, 2015, online edition.

Rid, Thomas. *Cyber War Will Not Take Place*. Vol. als eBook. New York City: Oxford University Press, 2013.

Rõigas, Henry, and Tomáš Minárik. "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law." Incyder News. Tallinn, Estonia: CCDCOE, August 31, 2015.

Roth, Andrew. "Russia and China Sign Cooperation Pacts." *New York Times*. May 8, 2015, online edition. http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0.

Schmitt, Michael N. "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis." *Lawfare Blog*, January 8, 2015. https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis.

———. "'Attack' as a Term of Art in International Law: The Cyber Operations Context." In *Cyber Conflict (CYCON), 2012 4th International Conference on*, 1–11. IEEE, 2012. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243981.

Schneier, Bruce. "Attack Attribution and Cyber Conflict - Schneier on Security.pdf." *Schneier on Security*, March 9, 2015. https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html.

———. "Computer Network Exploitation vs. Computer Network Attack." *Schneier on Security*, March 10, 2014. https://www.schneier.com/blog/archives/2014/03/computer_networ.html.

Selin, Sean. "Governing Cyberspace: The Need for an International Solution." *Gonz. L. Rev.* 32 (1996): 365. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gonlr32&section=18.

Shackelford, Scott J., J. D. Scott Russell, and Andreas Kuehn. "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors." *Kelley School of Business Research Paper*, no. 15–64 (2015). http://works.bepress.com/cgi/viewcontent.cgi?params=/context/scott_shackelford/article/1016/type/native/&path_info=.

Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford ; New York: Oxford University Press, 2014.

Sputnik International. "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official." *Sputnik International*, August 17, 2015, online edition.

http://sputniknews.com/politics/20150817/1025819426/UN-cybersecurity-report-compromises-on-self-defence.html.

Stahl, William M. "Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity, The." *Ga. J. Int'l & Comp. L.* 40 (2011): 247. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gjicl40&section=12.

Stavridis, James. "Incoming: What Is a Cyber Attack?" *Armed Forces Communications and Electronics Association Magazine*, January 1, 2015. https://www.afcea.org/content/?q=incoming-what-cyber-attack.

Tatam, Robin. "Cracking the Problem of Endpoint Security." Helpsystems, December 19, 2014. http://www.helpsystems.com/powertech/cracking-endpoint-security-problems.

Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008.

United Nations. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." New York, USA: United Nations, June 24, 2013.

———. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations, July 22, 2015.

Watts, Sean. "Cyber Norm Development and the United States Law of War Manual." In *NATO Cooperative Cyber Defence Centre of Excellence, International Cyber Norms Development*, by Anna-Maria Osula. Tallinn, Estonia: ATO Cooperative Cyber Defence Centre of Excellence, 2016.

[1] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/70/172, July 22, 2015.

[2] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/70/172, July 22, 2015; and *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Document A/68/152, June 24, 2013.

[3] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series,* 1, May 20, 2014, <http://dash.harvard.edu/handle/1/12308565>.

[4] *Proposal for an International Code of Conduct for Information Security*, Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, September 12, 2011.

[5] Julie Hirschfeld Davis and David E. Sanger, "Obama and Xi Jinping of China Agree to Steps on Cybertheft," *The New York Times*, September 25, 2015, < http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html>; and Andrew Roth, "Russia and China Sign Cooperation Pacts," *The New York Times*, May 8, 2015, < http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html>.

[6] "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official," Sputnik International, August 17, 2015, < http://sptnkne.ws/AYy>.

[7] United Nations 2015; Decision No. 1106: *Initial Set Of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies*, Organization for Security and

Co-operation in Europe Permanent Council, 1, December 3, 2013; and *ARF Work Plan on Security of and in the Use of Information and Communications Technologies*, ASEAN, May 7, 2015.

[8] Henry Rõigas and Tomas Minárik, *2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law*, NATO Cooperative Cyber Defense Centre of Excellence, August 31, 2015.

[9] United Nations 2015; Rõigas and Minárik.

[10] Sputnik International.

[11] Joseph Marks, "U.N. Body Agrees to U.S. Norms in Cyberspace," Politico, July 9, 2015, <http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900>

[12] Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," 2014 5th International Conference on Cyber Conflict, ed. K. Podins, J. Stinissen, M. Maybaum, 2013.

[13] Sean Selin, "Governing Cyberspace: The Need for an International Solution," *Gonzaga Law Review*, 365, 1996; Tim Maurer, "Cyber Norm Emergence at the United Nations," Science, Technology, and Public Policy Proram Explorations in Cyber International Relations Project, September 2011; Nye 2014; Paul Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict," *The Washington Quarterly*, 38 (2) pp. 47 - 61; and Sean Watts, "Cyber Norm Development and the United States Law of War Manual," *NATO Cooperative Cyber Defence Centre of Excellence, International Cyber Norms Development*, August 7, 2015.

[14] Paul Meyer, "Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace," *ICT for Peace Foundation*, September 4, 2015, <http://t.co/ccXFDvPW4O>.

[15] Scott Shackelford, Scott Russell, and Andreas Kuehn, "Unpacking the International Law on Cybersecurity Due Diligence," August 27, 2015, *Chicago Journal of International Law*, 2016; and William M. Stahl, "Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity," *Georgia Journal of International and Comparative Law*, 40 (1) 2011.

[16] Major Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Airforce Law Review*, 167 2012; and Bruce Schneier, "Attack Attribution and Cyber Conflict," *Schneier on Security*, January 8, 2015, <https://www.schneier.com/blog/archives/2015/01/attack_attribut.html>.

[17] Martin Libicki, "Would Deterrence in Cyberspace Work Even with Attribution," *Georgetown Journal of International Affairs*, April 22, 2015, <http://journal.georgetown.edu/would-deterrence-in-cyberspace-work-even-with-attribution/>.

[18] Robin Tatam, "Cracking the Problem of Endpoint Security," *Helpsystems*, December 19, 2014, <http://www.helpsystems.com/powertech/cracking-endpoint-security-problems>.

[19] Joseph S Nye Jr., "Nuclear Lessons for Cyber Security," DTIC Document, 2011, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA553620>.

[20] Bruce Schneier, "We Still Don't Know Who Hacked Sony," *The Atlantic,* January 5, 2015, <http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/>; and Bruce Schneier, "Reacting to the Sony Hack," *Schneier on Security*, December 22, 2014, <https://www.schneier.com/blog/archives/2014/12/reacting_to_the.html>.

[21] David Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say," *The New York Times,* January 18, 2015, <http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html>

[22] Schneier 2015.

[23] Kenneth Geers, Darien Kindlund, Ned Moran, and Rob Rachwald, "World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks," Technical report, FireEye, 2014, <http://ver007.com/tools/APTnotes/2013/fireeye-wwc-report.pdf>

[24] Nicolas Falliere, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier." *Symantec*, September 30, 2010.

[25] Ibid.

[26] Bruce Schneier, "Computer Network Exploitation vs. Computer Network Attack," *Schneier on Security*, March 10, 2014, < https://www.schneier.com/blog/archives/2014/03/computer_networ.html>.

[27] Joint Chiefs of Staff, "Cyberspace Operations," Joint Publication 3-12 (R), Washington D.C.: Department of Defense, February 5, 2013; and Joint Chiefs of Staff, "Information Operations," Joint Publication 3-13, Washington D.C.: Department of Defense, November 20, 2014.

[28] Schneier, "Computer Network Exploitation vs. Computer Network Attack."

[29] Nate Cardozo and Eva Galperin, "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?" Electronic Frontier Foundation, May 20, 2015, <https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation>; and Andrea Peterson, "The Government Is Headed back to the Drawing Board over Controversial Cybersecurity Export Rules," *The Washington Post,* July 29, 2015, <https://www.washingtonpost.com/news/the-switch/wp/2015/07/29/the-government-is-headed-back-to-the-drawing-board-over-controversial-cybersecurity-export-rules/>.
[30] John Arquilla, "Cyberwar Is Already Upon Us," *Foreign Policy*, February 27, 2012, <http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/>; Thomas Rid, *Cyber War Will Not Take Place*, Vol. als eBook (New York City: Oxford University Press, 2013); and P.W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (New York: Oxford University Press, 2014).
[31] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008).
[32] Rid argues that: ". . . all acts of war are violent or potentially violent . . ., an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker's will . . . to qualify as an act of war, an attack must have some kind of political goal or intention."
[33] Rid.
[34] James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," (Washington D.C.: Office of the Director of National Intelligence, February 26, 2015).
[35] Michael N. Schmitt, "'Attack' as a Term of Art in International Law," Proceedings of the 4th International Conference on Cyber Conflict, September 7, 2012, 283-293.
[36] James Stavridis, "Incoming: What Is a Cyber Attack?" *Armed Forces Communications and Electronics Association Magazine*, January 1, 2015, <https://www.afcea.org/content/?q=incoming-what-cyber-attack>; and Michael N. Schmitt, "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis," *Lawfare Blog*, January 8, 2015, <https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis>.
[37] Given the scope of this paper, the author will not go into further detail about the (legal) differences between the use of force and an armed attack in cyberspace. However, it is important to note that most scholars agree that the threshold under Art. 2(4) UN Charter is lower than under Art. 51 of the UN Charter. In other words, a particular cyber attack might breach Art. 2(4) but not rise to the threshold of allowing a state to invoke self-defense under Art. 51.
[38] United Nations, *Charter of the United Nations*, October 24, 1945, 1UNTS XVI.
[39] NATO, *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* Ed. Michael N. Schmitt. (Cambridge: Cambridge University Press, 2013).
[40] *Proposal for an International Code of Conduct for Information Security*.
[41] United Nations 2013.
[42] United Nations 2015.
[43] Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict."
[44] Meyer, "Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace."
[45] Nye, "The Regime Complex for Managing Global Cyber Activities."
[46] Patryk Pawlak, "Cyber Diplomacy," Briefing, Brussels, Belgium: European Parliament, October 2015. 2.
[47] Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, 39(3), Winter 2014/2015, 7-47; and Sophie Beach, "China and Russia Support 'Cyber Sovereignty,'" *China Digital Times*, May 11, 2015, <http://chinadigitaltimes.net/2015/05/china-and-russia-agree-to-respect-cyber-sovereignty/>.
[48] *Proposal for an International Code of Conduct for Information Security*
[49] *Department of Defense Dictionary of Military and Associated Terms*, Department of Defense, Joint Publication 1-02, 58.
[50] *Submission to the United Nations General Assembly Resolution*, Permanent Representative of the People's Republic of China, A/62/98, May 15, 2007, 7.
[51] Ashley Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process," *Lawfare Blog*, May 31, 2015, <https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process>.
[52] Maurer; Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law," *Texas Law Review,* 88 (2009): 1571, <http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr88&section=56>;

Watts, "Cyber Norm Development and the United States Law of War Manual"; Selin; and Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," *American Foreign Policy Interests,* 36(5), September 3, 2014, 322–31.

[53] United Nations 2013.

[54] Pawlak.

[55] For more general information and latest proposals on CBMs in cyberspace, see: Healey et al., "Confidence-Building Measures in Cyberspace - A Multistakeholder Approach for Stability and Security."

[56] Organization for Security and Co-operation in Europe Permanent Council.

[57] Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict."

[58] Nye Jr, "Nuclear Lessons for Cyber Security."

[59] New America, Global Cyber Definitions Database, <www.newamerica.org/cyber-global/cyber-definitions/>

[60] See: https://www.cybersecurity.ox.ac.uk/education/cdt.

[61] See: http://www.lawandsecurity.org/ASPIRE-Scholarship.