Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Manuel Fischer, *Connections QJ* 18, no. 1-2 (2019): 69-92
https://doi.org/10.11610/Connections.18.1-2.05

Research Article

The Concept of Deterrence and Its Applicability in the Cyber Domain

Manuel Fischer

George C. Marshall European Center for Security Studies,
http://www.marshallcenter.org

Abstract: Cyberspace as the fifth domain is omnipresent, and all developed states increasingly realize that international relations and typical domains of statehood change in the face of global digitization. With the advent of game-changing technologies, traditional statecraft tools, such as deterrence, seem disregarded as outdated in the national security strategy building process. Advanced states, in particular, depend heavily on an open and safe cyber domain but, at the same time, suffer from manifold vulnerabilities. The recent past showed that sophisticated cyberattacks have the potential to disrupt governments, economies, and societies significantly and therefore pose a threat to core security interests. As a classical tool in international relations, deterrence can help bolster national security interests, even if the cyber domain requires some special considerations. Therefore, the article explains the basic mechanisms of deterrence in the nuclear age and contemporary international relations, cyberspace's legal framework, and possible ways to apply deterrence in the cyber domain. It aims to urge global leaders to thoroughly consider deterrence in the cyber domain as a powerful asset and to provide policymakers with options for action.

Keywords: cybersecurity, cyber operations, deterrence, legal framework

Introduction

Speaking about deterrence in the 21st century feels like excavating remnants of a bygone era. With the advent of nuclear technologies and mainly during the Cold war, deterrence was a topic not only for politicians and academia but also shaped the daily lives of millions, no matter which side of the 'blocks' they belonged to. Since then, deterrence diminished its presence in the public percep-

tion together with the nuclear arsenals of the great powers. What remains is still of enormous potential but as a tool of statecraft rather than a placeholder.

Especially states face the gradual change of the traditionally state-centered setting of the international system, particularly in habitual domains of statehood, like security. The classical understanding of war and conflict blurs and the traditional state structures seem to be overstrained to respond with the classical tools, as the new type of conflict is multilayered (political, military, and economic, among others), conducted mostly by non-military means like propaganda and political agitation and amongst diverse state and non-state actors.[1,2]

In the face of daily and continuing attacks on governments and their organs,[3] the question persists: What keeps an actor in the cyber domain from carrying out the same attacks over and over again, or even climbing up the escalation ladder and causing irreversible harm, if it serves his interests. There seems to be no respect, no fear of retaliation, and no serious technical barriers in the cyber domain – or in other words, no deterrence.

This article will survey if the concept of deterrence is only effective if it is tied to nuclear weaponry and if it becomes useless in a no longer (purely) nuclear but cyber-dominated international system. The author claims that this is not the case! Even in the cyber age, deterrence can be a powerful tool of statecraft and could contribute to the protection of state's national security interests. To prove this hypothesis, this article will scrutinize the concept of deterrence by looking into the past that generated manifold experiences on that topic, to finally project the findings into present times. Therefore, existing concepts of deterrence and special implications of the cyber arena, together with the legal framework of the ever more digitized international system, will be examined to finally find effective ways to apply deterrence in cyber space.

---

1 David J. Betz, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (London and New York: Routledge, 2017), 80.

2 Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, quote on p. 48, https://doi.org/10.1162/ISEC_a_00266.

3 Like it happened in Germany in 2015, when a Russian hacker group called "Fancy Bear" attacked the German Parliament, spied on at least 16 members (including Angela Merkel) and extracted several partly confidential documents. By that time, the Federal Chancellery spoke about (hybrid) warfare and potential counterstrikes for the first time since decades. See Patrick Beuth, Kai Biermann, Martin Klingst, and Holger Stark, "Bundestags-Hack – Merkel und der schicke Bär," *Zeit Online*, May 10, 2017, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland. And yet, the same happened again in late 2017, when security officials detected a presumably Russian originated "Advanced Persistent Threat" aimed at the foreign ministry, which compromised the network for up to a year. See Thorsten Severin and Andrea Shalal, "German Government under Cyber Attack, Shores up Defenses," *Reuters*, March 1, 2018, https://www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8.

The following assumptions and exclusions are considered common ground:

- The emerging fifth-generation mobile technology (5G) and cloud technologies will boost the spreading of the Internet of Things. Critical processes will be gradually transferred to these technologies and cyber risks will rise exponentially as the new devices create more opportunities for potential breaches. Plus, by controlling physical assets, even physical harm can be caused.[4,5]
- According to the "Assume-Breach-Paradigm," it is highly likely that every sufficiently complex software product has critical vulnerabilities and that updates are either not provided or the vulnerability is kept secret.[6]
- This research will focus on political cyber threats and cover criminal cyber activities only as far as they occur in the context of conflict. Traditional espionage via cyber means will be excluded from this research.

Mechanisms of Deterrence

The concept of deterrence is as old as mankind's craving for fighting each other.[7] The term "deterrence" is derived from the word "terror," which reflects the fear of costs that are related to a certain action. In academic literature, sometimes the term "dissuasion" appears to indicate the broader range of measures, which are not only focused on inflicting costs but also on denying benefits for the adversary.[8] For the sake of a clear distinction and in view of the dominating use in the political and academic realm, this work will use "deterrence" as an umbrella term, aware of the fact that the concept is much broader.

Joseph Nye also takes both denotations into account by defining deterrence as[9]

> … dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit.

---

4 "BSI: Critical infrastructures – Definition," Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance, 2017, www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html.

5 James Manyika, et al., *The Internet of Things: Mapping the Value beyond the Hype* (McKinsey & Company, June 2015), 11.

6 "BSI: Critical Infrastructures," 18.

7 Early references date back to Thucydides' work about the Peloponnesian War, even before the Christian calendar emerged, see Richard Ned Lebow, "Thucydides and Deterrence," *Security Studies* 16, no. 2 (2007): 163–188, quote on p. 163 https://doi.org/10.1080/09636410701399440.

8 Michael Quinlan, "Deterrence and Deterrability," in *Deterrence and the New Global Security Environment*, ed. Ian R. Kenyon and John Simpson (London: Routledge, 2006), 5.

9 Nye, "Deterrence and Dissuasion in Cyberspace," 45.

This means to preserve the status quo by preventing an opponent from conducting a course of action that is viewed as unfavorable. It is not about compelling the adversary to certain behavior and thereby altering the status quo.[10] Considering key mechanisms and the application in International Relations (IR) will help to understand the common ground and lead the way to cyber deterrence.

According to the deterrence theorists Sir Michael Quinlan,[11] there is "no such thing as an undeterrable state."[12] As basic prepositions for successful deterrence (no matter in which realm), he considers the following five points[13]:

1. Probabilities
2. Capability and a credible intent
3. Deterrence declaration
4. Prospect to cause multifaceted costs
5. Using the whole range of possible responses.

Probabilities

Ideal deterrence would work with certainties, for example, "if you take my lunch, I will destroy your toy." But as human interaction is of a rather complex nature, several uncertainties emerge, and misperception and misinterpretation are unavoidable. To face that, probabilities need to be considered.[14] Not only the potential gain value ("lunch") and loss value ("toy") play a relevant role, but also the probability of succeeding or losing. As a consequence, the dimensions of gain probability ("you can't be sure to get my lunch because I will try to defend it") and loss probability ("if you take my lunch, I will do my best to destroy your toy and maybe I will succeed") need to be added to the following decision calculus[15,16]:

*Gain Value * Gain Probability < Loss Value * Loss Probability*

---

[10] Wyn Q. Bowen, "Deterrence and Asymmetry: Non-state Actors and Mass Casualty Terrorism," *Contemporary Security Policy* 25, no. 1 (2004): 54-70, https://doi.org/10.1080/1352326042000290506.

[11] Former Permanent Under-Secretary of State at the British Ministry of Defense; influential defense and deterrence strategist.

[12] Quinlan, "Deterrence and Deterrability," 7.

[13] Quinlan, "Deterrence and Deterrability," 4.

[14] Quinlan, "Deterrence and Deterrability," 4.

[15] Philip Bobbitt, *Democracy and Deterrence: The History and Future of Nuclear Strategy* (Basingstoke: Palgrave Macmillan, 1988), 8.

[16] Jeffrey R. Cooper, "A New Framework for Cyber Deterrence," in: *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Georgetown University Press, 2012): 105-120, 109.

An effective deterrence in an uncertain environment needs to address all four factors of the inequation to ensure that the left part stays smaller than the right part in the adversary's perception.

Capability and a Credible Intent

Capabilities are the basis for an adversary to calculate the value he could gain and lose. However, there is also a need for a credible intent of using these capabilities to affect the calculation of probabilities.[17] Powerful offensive measures can increase the loss value, the credibility of offensive and defensive measures can change the calculation of probability of gain and loss.

*Gain Value * Gain Probability (↓) < Loss Value (↑) * Loss Probability (↑)*

Whereas capabilities are rather a matter of money, a credible intent can only be proven by action, but still, both need a "show of force" to be perceived by an opponent.[18]

Deterrence Declaration

Besides capability and credibility, the effective communication of the right deterrence message to the right audience is of significant importance.[19,20] Therefore, it is vital to state what actions will not be allowed to stand, that (offensive or defensive) capabilities for an appropriate reaction are at hand and that these will be employed.[21] Hereby, an over-exact, self-limiting specification is unnecessary and can even be detrimental, as it opens the path for the adversary to evade or head off a response.[22] Effective communication gives the adversary distinct factors for his calculation and reduces misinterpretations or misperceptions. Furthermore, a strong deterrence declaration can per se affect the perception of gain and loss probability.

---

[17] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, Maryland: Rowman & Littlefield, 2017), 9.

[18] The US showed a new capability in the 1989 invasion of Panama by employing the F-117 Stealth fighter-bomber, surely not because of the threat of the Panamanian air defenses but to demonstrate a new capability in the toolbox, see Richard A. Clarke and Robert K. Knake, *Cyber War: What It Is and How to Fight It* (New York: HarperCollins, 2010), 194.

[19] Bowen, "Deterrence and Asymmetry," 51.

[20] Jasper, *Strategic Cyber Deterrence*, 9.

[21] Although a defined red line is missing, the U.S. provides a good example by publicly asking IT-contractors to compete for a nearly $ 500M contract to develop and, if necessary, deploy lethal cyber weapons. The executive director of U.S. Cyber Command stated that the U.S. is looking for loud offensive cyber tools that can be traced back to the United States. See Jasper, *Strategic Cyber Deterrence*, 102.

[22] Quinlan, "Deterrence and Deterrability," 4.

*Gain Value * Gain Probability (↓) < Loss Value * Loss Probability (↑)*

Current experts, like the former US undersecretary of defense for policy, James Miller, point out that, "[y]ou don't really deter states, you deter individuals and group decision-makers…"[23] This means that the deterrence declaration needs to be designed reversely, starting with the desired effect, and considering how it will be processed by those it should deter.[24] The assumption that an adversary acts rationally is rather simplified, as it would require perfect information and the willingness to take decisions only based on its strategic implications. Decision-makers never have perfect information and are influenced by many factors like emotions or personal interests.[25]

Prospect to Cause Multifaceted Costs

By building up defensive structures, the desired effect can be denied or at least mitigated. This will sow the seed of doubt in the adversary's mind as he needs more time and resources, and the probability of detection rises.[26] In short, denial measures increase the opportunity costs of the challenger. Combining retaliation and denial measures and increasing the variety of costs makes it harder for the opponent to prepare and harden its values in advance.[27] Thus, both the loss value and the loss probability rise.

*Gain Value * Gain Probability < Loss Value (↑) * Loss Probability (↑)*

To increase this effect, it can be expedient to tailor a strategy to a specific adversary. This demands contextual knowledge of the actor's motives, decision-

[23] Sean D. Carberry, "Why There's no Silver Bullet for Cyber Deterrence," *Federal Computer Week (FCW)*, June 06, 2017, https://fcw.com/articles/2017/06/06/carberry-cyber-deterrence.aspx.

[24] How an opponent interprets a deterrence declaration depends on their history and strategic culture and is a source of misinterpretation based on different preferences and expectations. See James Andrew Lewis, "Rethinking Deterrence," Report (Washington: Brzezinski Institute on Geostrategy, May 2016), 5, https://csis-website-prod.s3.amazonaws.com/s3fs-public/170713_Deterrence_Stability_0.pdf.

[25] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–135, 107, https://www.hsdl.org/?view&did=18663.

[26] Bowen, "Deterrence and Asymmetry," 50.

[27] Such a combination of retaliation and denial aspects was to be seen under the George W. Bush administration for deterring the use of unconventional weapons by regimes of concern through combining denial capabilities (development of a comprehensive missile defense) and the threat of overwhelming punishment. See Bowen, "Deterrence and Asymmetry," 50.

making processes, and command and control structures and would mean a high intelligence effort and cultural understanding.[28]

Using the Whole Range of Possible Responses

If the costs displayed do not match the means or magnitude of the actions attempted to prevent, even opponents of different sizes and value-systems can be deterred.[29] Using the entire range of possible responses makes it harder for the adversary to predict an answer and protect himself. Thus, the loss value, as well as the loss probability, can be increased.

*Gain Value * Gain Probability < Loss Value (↑) * Loss Probability (↑)*

As a state usually holds the monopoly on the use of force and possesses a wide range of kinetic means, this can be an advantage in facing non-state opponents. Switching the domains of response to classical and familiar grounds of statehood can strengthen legitimacy and credibility.[30]

Special Implications of the Cyber Domain

Ever since states and governments engaged with each other in the arena of IR, deterrence used to be a valuable tool. The most influential era of deterrence emerged with the advent of nuclear weapons and essentially defined the Cold War course. There are parallels to the cyber age, which can provide valuable help, but there are also aspects that must be disregarded.

The 1945 atomic bombing of Hiroshima and Nagasaki suddenly forced the world to face a new military capability that was perceived as unstoppable and producing non-survivable effects. It took strategists several years to come from NATO's so-called "massive retaliation" over the turning points of the Sputnik-Shock and the Cuba-Crisis and the subsequent deterrence concept of "mutual assured destruction" to the comprehensive strategy of "flexible response." That was a graduated concept, escalating from conventional defense to the strategic employment of nuclear weaponry. It was based on capability (conventional and nuclear forces) and at least some credibility (the US nuked Japan), relying on the whole range of means (from conventional response to tactical and strategic nuclear means) to promise multifaceted costs (strikes against military and eco-

[28] Bowen, "Deterrence and Asymmetry," 51.

[29] Quinlan, "Deterrence and Deterrability," 4.

[30] When the Islamic State's propaganda machine became too strong and uncontrollable, the U.S. government turned to lethal force in the shape of air-strikes against high-level media division operatives which became legitimate targets in an armed conflict due to their affiliation with the terrorist group. See Jasper, *Strategic Cyber Deterrence*, 95.

nomic targets on the battlefield and in the homeland), but it was not self-limiting in the ways of response (no predefined escalation-ladder).[31]

This well-defined strategy indeed brought a certain stability to the international system and was based on five factors that characterized the then modern concept of war (and thus of deterrence) in the face of new and complex technology[32]:

1. *Time factor:* Excessive harm could now be done in a short time, with hardly any prewarning.
2. *Force factor:* Immediately available forces outrivaled mobilization forces due to the time factor.
3. *Survival factor:* A first excessive strike needed to be survived to launch a counter attack.
4. *Globalization factor:* A nuclear war would escalate globally immediately.
5. *Defense factor:* NATO's defense needed to be based on displaying strengths, not on protecting weaknesses.

NATO is still a nuclear alliance (mainly based on the US capability and credibility), and nuclear deterrence remains a part of its defense strategy. Nonetheless, since the Cold War, the world's atomic arsenals got systematically reduced, and various non-nuclear technologies emerged. Some even say that in the context of powerful alternatives, nuclear weapons are relegated to a passive and symbolic role in IR.[33] At the same time, the vertical[34] and horizontal[35] proliferation of destructive technologies became easier to conduct and harder to control.[36]

But even if the concepts of nuclear deterrence cannot be copied, it is still possible to learn how a complex strategy for the use of new and overwhelming

---

[31] "Nuklearstrategie – Zwischen Abschreckung und Einsatzdoktrin," *Bundeszentrale für politische Bildung*, https://sicherheitspolitik.bpb.de/m6/articles/nuclear-strategy-between-deterrence-and.

[32] Bruno Thoß, *NATO-Strategie und nationale Verteidigungsplanung: Planung und Aufbau der Bundeswehr unter den Bedingungen einer massiven atomaren Vergeltungsstrategie 1952 bis 1960* (München: Oldenbourg Verlag, 2006).

[33] Lewis, "Rethinking Deterrence," 5.

[34] Increase in number and sophistication of weapons of established weapon holders. See Ian R. Kenyon and John Simpson, eds., *Deterrence and the New Global Security Environment* (Abingdon: Routledge, 2006).

[35] Dissemination of nuclear technology to others. See Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

[36] In fact, the established nuclear powers are concerned that their nuclear deterrence might be circumvented or beheaded by advanced conventional weapons. These would not reach the nuclear threshold and thereby a strike of the level of a nuclear attack against vital values could stay unpunished, See Lewis, "Rethinking Deterrence," 4.

technologies can be developed.[37] In parallel with the nuclear age, the cyber age stands for the development of a new, man-made, and hard to grasp technology that has overwhelming potential for civil use and, at the same time, for unimaginable destruction. These common features enable the assumption that the same factors as in nuclear deterrence play at least a basic role in cyber deterrence. The following paragraph will examine the previously introduced implications of time, forces, survival, globalization, and defense in the cyber domain and will add the cyber specific factor of attribution to the set of aspects.

Time Factor

In the cyber age, the time factor for the attack itself seems to tend to zero as Artificial Intelligence employs algorithms to take over basic, but time-consuming tasks, and actors all around the world are connected in milliseconds. This so-called "net-speed" creates a simultaneity of cause and effect that ceases the need to costly and difficultly bridge distance. Now even small actors can affect states without any prewarning.[38] However, this only holds true for the attack itself. Similar to the Cold war, the preparation of the battlefield is a necessary precondition to attack in net-speed. Like identifying command bunkers, an advanced cyber attacker needs to infiltrate and map a system, gain access and place backdoors.[39,40] This means a long-term campaign, which cannot be conducted entirely from behind a computer but consists of complex human intelligence (HUMINT) operations.[41]

Force Factor

Immediately and constantly available forces with the latest technological knowledge and equipment outrivaled mobilization forces due to the time factor. Still, governments use the same concepts as for noncyber attacks by delegating defensive tasks and deterrence duties against small actors to local police forces and employing federal agencies only against state actors or terrorist groups.[42] This means fragmentation of responsibilities and an incoherent strategy. Simultaneously, technological knowledge and equipment cost immense amounts of money and require agile and specialized structures. Both are only available to a

---

[37] Clarke and Knake, *Cyber War: What It Is*, 155.

[38] Betz, *Cyberspace and the State*, 39.

[39] Richard B. Andres, "The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 89–104.

[40] Clarke and Knake, *Cyber War: What It Is*, 30.

[41] Jeffrey Carr, "Responsible Attribution: A Prerequisite for Accountability," Tallinn Paper No. 6 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014).

[42] Andres, "The Emerging Structure of Strategic Cyber Offense," 91.

certain extent in governments, and therefore an increasingly significant role falls to the private sector.

Special focus falls to the supply chain of IT soft- and hardware. Often cybersecurity and data protection issues are not considered in the invention stage and the ex-post fixing of vulnerabilities is not always possible.[43] By compromising hardware in an early stage of development, vulnerabilities can be created and easily distributed up the supply chain.[44] This brings into focus the whole chain, down to the smallest "smart valve." Although such targets may sound insignificant, it has been evaluated that especially highly sophisticated threat agents concentrate on them.[45] Thus, it has become crucial to determine who manufactures, tests, and certifies hardware, where spare parts come from, and which manufacturing and distribution processes need to be under constant national control.

Survival Factor

Being able to survive the first strike and staying able to act was a key element in the nuclear setting. The cyber domain as well seems to be an offence-dominated environment in which attackers have a structural advantage over defenders, and definite protection is not possible. Moreover, industrialized and connected countries seem to be more vulnerable than less advanced ones.[46,47] This leads to a nuclear-era-like self-deterrence of the powerful, industrialized, and connected states. Being aware of their own cyber vulnerability, a reluctance to use the usual superiority in other areas (like conventional weapons) emerges.[48] As it seems impossible to reduce the level of interconnectedness in modern societies, the best option is to improve deterrence and defenses.[49]

---

[43] ENISA, "Threat-Landscape-Report 2017" (Heraklion: European Union Agency for Network and Information Security), 107, www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport.

[44] This phenomenon is not exclusively linked to the cyber domain. For years, the U.S. Department of Defense (DOD) struggles with counterfeit parts in its critical defense supply chains. See United States Government Accountability Office (GAO), "Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk" (Washington D.C.: US GAO, 2016), https://www.gao.gov/products/GAO-16-236.

[45] ENISA, "Threat-Landscape-Report 2017," 110.

[46] Jack L. Goldsmith, "How Cyber Changes the Law of War," in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, ed. Frederic Lemieux (London: Palgrave Macmillan, 2015), 51–61.

[47] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (January 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

[48] Clarke and Knake, *Cyber War: What It Is*, 157.

[49] Clarke and Knake, *Cyber War: What It Is*, 149.

Globalization Factor

Like nuclear war, cyberattacks ignore the barriers and borders in the real world. An attacker no longer needs to be near the scene or in reach of the defenders.[50] Net-speed collapses spatial distance to zero and allows actors outside a state's jurisdiction to exercise power against it with a good chance of never getting prosecuted.[51] This leads to a global cyber arena, where state actors are often bound by jurisdictions whereas their attackers evade their grasp easily.[52,53] Even more than in the nuclear age, such attacks can have a wide spectrum of effects that makes its scale hard to predict. A cyber tool like a virus can bounce back, spread to other countries, or create unpredictable global havoc in minutes.[54]

A further aspect of a globalized arena is the geopolitical symmetry, even for states not neighboring each other. If a state does not possess the escalation dominance (a favorable asymmetry of power and means), it might struggle to appropriately retaliate as it must fear to lose the escalations series in the end in the physical domain.[55]

Defense Factor

Unfortunately, the cyber realm lacks clear norms of what a proper defense and what an appropriate response are.[56,57] Besides the fact that cyber conflict skips the traditional battlefield and takes place in every-day systems (e.g., banks, television, and air traffic management,[58] the biggest challenge for deterrence is that offensive and defensive capabilities are kept under a code of silence. On the one hand, an opponent can prepare its own defense if he knows the adversary's offense and, on the other hand, there is no incentive to disclose a breach as it might ruin the reputation of the victim. Thus, there is no chance of learning from others and developing proper defense tools.[59] In the context of deterrence, this is counterproductive (as constant communication of clear and targeted deterrence decelerations is key) and must be overcome with a compromise of keeping

---

50 Goldsmith, "How Cyber Changes the Law of War," 53.

51 Betz, *Cyberspace and the State*, 39.

52 Clarke and Knake, *Cyber War: What It Is*, 30.

53 Andres, "The Emerging Structure of Strategic Cyber Offense," 92.

54 Goodman, "Cyber Deterrence," 116.

55 Estonia was reluctant to attribute the 2008 cyberattacks to Russia (even if it had good evidence) because of the geopolitical imbalance and the possible physical escalation of the far superior Russian military. See Goodman, "Cyber Deterrence," 109.

56 Carberry, "Why There's no Silver Bullet for Cyber Deterrence."

57 Andres, "The Emerging Structure of Strategic Cyber Offense," 101.

58 Clarke and Knake, *Cyber War: What It Is*, 30.

59 Andres, "The Emerging Structure of Strategic Cyber Offense," 93.

secret as much as possible but disclosing and communicating enough to effectively deter.[60]

Attribution Factor

Attribution was not a big issue in the nuclear age and, even today, with only nine states possessing nuclear weapons and well-known isotopic identifiers of each arsenal, it is a matter of minor concern.[61] But unlike nuclear weapons, cyber means are harder to trace back, and the hundred percent attribution to an originator is seldom possible.[62] The opinion is widespread that this thwarts the concept of deterrence, but in fact, even with an imperfect attribution, deterrence is possible, as long as three audiences are addressed[63]:

1. *The defending government* wants a relatively high assurance from its intelligence agencies and network forensics;
2. *The attacking government or non-state actor* knows what has been done but cannot be sure how good the opposing forensics and intelligence are; even if it denies the attack, it will never know how credible this deception was;
3. *The domestic and international public* needs to be convinced of the justice of retaliation. Therefore, a certain degree of detail needs to be disclosed, even if forensic methods can become useless for future cases.

The quality of attribution is a function of available resources, available time, and the adversary's sophistication. The less top-end forensic skills and highly experienced personnel are available, the lower the attribution quality will be. The higher the time pressure for attribution, the lower the quality will be. The more experienced and well-funded an opponent is, the lower the quality of attribution will be.[64]

Today it is less a question of *if* it is possible to attribute a cyberattack, but rather *how long* it will take.[65] As long as all cyberattacks follow the Cyber-Kill-Chain pattern[66] and involve a human adversary, there will be mistakes, individ-

---

[60] Goodman, "Cyber Deterrence," 109; Andres, "The Emerging Structure of Strategic Cyber Offense," 101.

[61] Nye, "Deterrence and Dissuasion in Cyberspace," 50.

[62] Clarke and Knake, *Cyber War: What It Is*, 68.

[63] Nye, "Deterrence and Dissuasion in Cyberspace," 51.

[64] Rid and Buchanan, "Attributing Cyber Attacks," 32.

[65] Tim Maurer, "Here's How Hostile States Are Hiding behind 'independent' Hackers," *The Washington Post*, February 1, 2018, www.washingtonpost.com/news/monkey-cage/wp/2018/02/01/heres-how-hostile-states-are-hiding-behind-independent-hackers.

[66] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1, no. 1 (2011):

ual motivations, and relationships that make the tracing, fighting and deterring possible.[67] This fact brings up another parallel to the nuclear age. Dealing with humans cannot be done virtually or from behind a computer. The best way to attribute an attack after it happened is to already have an intelligence campaign of infiltration and trusted contacts in place.[68] This rather traditional HUMINT intelligence techniques become important again and may outpace the recently preferred and convenient signal intelligence (SIGINT).[69]

Legal Framework of Cyber Space

Like the advent of nuclear weapons, the information age brought game-changing modern technologies that altered the way IR and their legal frame were to be seen. Some even argue that these new technologies outpaced law and that recent legislation cannot fully govern emerging cyber capabilities.[70,71] But as isolated solutions of single actors cannot work, only International Law (IL) is able to provide a legal framework. It still tries to grasp the implications of a digitized world and needs time to translate it into a cyber-specific treaty and customary law. Until then, cyberspace's escalation potential stays significant, as states can rely on leeway by resorting to differing interpretive positions.[72] The only way to reduce this destructive potential is to provide a stable and accepted legal framework.

In 2013, the UN's Group of Governmental Experts agreed that International Law—and in particular the Charter of the UN—is applicable in the cyber do-

1–14, 5, www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

67 "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," Complimentary Report (Milpitas: FireEye Inc., June 2014), www.iqpc.com/media/1003877/33776.pdf.

68 Carr, "Responsible Attribution," 8.

69 Clarke and Knake, *Cyber War: What It Is*, 215.

70 This reaches relevance in the context of the "Presumptive Legality" of International Law, which says that acts that are not forbidden are permitted. As modern information technologies are not explicitly considered in International Law, there is a lot of leeway for states as long as the gaps are not closed by custom law or explicit treaties. See Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York, NY: Cambridge University Press, 2016), 51, Rule 11.9.

71 Michael N. Schmitt, "The Law of Cyber Targeting," Tallinn Paper No. 7 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/uploads/2018/10/TP_07_2015.pdf.

72 Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No. 5, Special Expanded Issue (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf.

main.[73] This groundbreaking position by an internationally recognized body was the first crucial step to fill the legislative vacuum in cyberspace. It was accompanied by the release of the "Tallinn Manual on the International Law Applicable to Cyber Warfare" and followed by the Tallinn Manual 2.0 in 2017, which were drafted as non-binding studies under the leadership of the NATO CCDCOE.[74] The EU even went beyond that opinion by stating in its Cyber Security Strategy that "the same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain."[75]

Accordingly, for all states, the rules of engagement in the cyber arena are defined by IL's conditions, and to find an effective and credible deterrence position, the following points need clarification:

- How to classify a cyberattack under international law?
- What kind of response to a cyberattack is lawful?
- Which targets are lawful in a cyber-exchange?

Classification of a Cyber-Attack under International Law

The Tallinn Manual 2.0 states that "the principle of state sovereignty applies in cyberspace," and thus, a state can take all measures not prohibited by IL that it considers necessary and appropriate to deal with its cyber infrastructure, with actors in the cyber domain or with cyber activities within its territory.[76,77] Consequently, every hostile cyber operation aimed against a state's cyber and non-cyber infrastructure means a violation of sovereignty if physical harm or injury is caused.[78] This is not the case if an attack manipulates or deletes databases to cripple the economy or to influence political processes. Although several schol-

[73] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (United Nations General Assembly, 2015), 12, https://digitallibrary.un.org/record/799853.

[74] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/.

[75] Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels: European Union, 2013), 3, https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en.

[76] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: NATO Cooperative Cyber Defence Centre of Excellence, 2017), 11.

[77] Cited in Jasper, *Strategic Cyber Deterrence*, 142.

[78] Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law*, 54, (2014): 697-732.

ars demand to include these non-physical effects, they are still out of scope in the common interpretation.[79]

Cyber operations are non-kinetic in nature, and therefore often misperceived as non-forceful, although their effects can range from simple annoyance to death. Thus, cyberattacks need to be assessed according to their effects on the real world, and if they have an outcome comparable to a kinetic attack, they constitute a "use of force."[80,81] However, a state is only allowed to conduct forceful defensive actions in the case of an "armed attack," which means the use of force must reach a certain threshold.[82,83] This edge sometimes is kept in a strategic ambiguity to make the prediction of potential self-defense actions harder for the adversary.[84] The Tallinn Manual 2.0 becomes concrete only for acts of cyber intelligence gathering, cyber theft, and brief interruption of non-essential services, which do not qualify as armed attacks due to the lack of serious injuries or deaths or the cause of severe damage.[85,86] For attacks that do not reach the threshold of an armed attack but that are an unlawful use of force, only countermeasures aimed to stop the attack are utilizable.[87] If the use of force mounts

---

79 Michael N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova Law Review* 56, no. 3 (2011): 569-605, 574; Schmitt and Vihul, "The Nature of International Law Cyber Norms," 17.

80 The UN Charter prohibits the use or threat of force by demanding: "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." See United Nations, "Charter of the United Nations" (United Nations, 2016), Article 2 (4).

81 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 573.

82 This can also be the case, if a series of cyber incidents (that individually would fall below the threshold of an armed attack) aggregate. Therefore, they must have the same originator, must be related, and taken together must have the requisite scale. see Schmitt, *Tallinn Manual on the International Law*, 56, Rule 13.8.

83 United Nations, "Charter of the United Nations," Article 51.

84 In line with that, the 2014 NATO Summit in Wales decided to determine if a cyberattack would lead to the invocation of article 5 (and thus, be considered as armed attack) on a case-by-case basis. See Schmitt and Vihul, "The Nature of International Law Cyber Norms," 26. In the opinion of Lewis, "Rethinking Deterrence," 9, this strategic ambiguity of thresholds creates confusion and dilutes the deterrence effects. The NATO nuclear strategy of "Flexible Response" in contrast, held its escalation ladder in a strategic ambiguity (aware that the capabilities were known anyway) but made the redlines very clear. See Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

85 Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, 339.

86 Cited in Jasper, *Strategic Cyber Deterrence*, 142.

87 The Tallinn Manual 2.0 states in rule 20 that states are entitled to take countermeasures (cyber or non-cyber) in response to the breach of international legal obligation by another state. Rule 69 says that cyber operation constitutes a use of force if they

to an armed attack, carried out through the instrument of classic military force causing or risking destruction of property and injury or death, then forceful defensive action is permitted. Should the cyber operation be a component of an overall military action, it constitutes an armed attack, even if it independently would not qualify as such.[88] Consequently, states have an incentive to quickly treat pure cyber operations as an armed attack to justify a forceful defensive response, increasing the likelihood of escalation significantly.[89]

Lawful Responses to a Cyber-Attack

A state that falls victim to an unlawful cyber operation has certain rights under international law if the attack reaches at least the level of the use of force. This starts with the always lawful claim for compensations for physical or financial losses and non-forceful responsive actions like blocking incoming data transmissions. Above that, typical technical, political, or economic countermeasures aiming at cessation and reparation can be taken in response to an identified use of force. These measures can involve a limited degree of military force and would normally be contrary to international obligations, but are lawful if proportionate to the injury suffered and below the threshold of an armed attack. However, the opposing state needs to be called in advance to refrain from going on or to take measures to stop acts emanating from its territory.[90,91] The right to take countermeasures is reserved for states, even if there are private IT-companies with cyber capabilities that exceed the state's arsenal. Nevertheless, the Tallinn Manual 2.0 explicitly mentions the right of an injured state to turn to private firms to conduct cyber operations on its behalf. Of course, the responsibility for the countermeasures conducted by the privateer stays with the state.[92,93]

If the use of force mounts to the level of an armed attack (no matter if initiated by a state or a non-state actor), the right of self-defense applies, and necessary and proportionate forceful actions can be conducted against an attacking

---

have comparable effects like non-cyber operations that would qualify as use of force. Countermeasures in this case can only be aimed to remedy existing harm as long as the threat exists and not for retaliation purposes. Furthermore, the adversary has to be warned in advance to give him the chance to cease the attack. See Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, cited in Jasper, *Strategic Cyber Deterrence*, 174.

88 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 587.

89 The US approach in this matter bears exactly this danger but seems to be effective in the cyber arena, as all uses of force are considered as armed attack and may be answered forcefully. See Schmitt, "'Below the Threshold' Cyber Operations," 730.

90 Schmitt, *Tallinn Manual on the International Law*, 36, Rule 9.

91 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 581.

92 Schmitt, "'Below the Threshold' Cyber Operations," 727.

93 Jasper, *Strategic Cyber Deterrence*, 179.

opponent.[94] As there is no international consensus on the borderline between the use of force and armed attack, this becomes a matter of interpretation and persuasive power of the injured state, as IL does not dictate the level of certainty of attribution to act in self-defense.[95] The question arises, how to respond to non-state actors, which, per definition, cannot violate the prohibition of the use of force under the international law made for states. In such cases, state responsibility offers an option to apply IL anyway. A state is not only responsible for the actions of its governmental organs but also for the conduct of individuals or groups that act on the instructions or under the control of the state.[96] Furthermore, a state can be held responsible for unlawful acts of non-state actors in its territory if it fails to take appropriate measures to stop the attack or provide all available support to investigate the incident.[97,98] If this state is unwilling or incapable to fulfill its legal duty, the victim state can act in self-defense and stop the attack with kinetic or cyber means, even on the other state's territory. But self-defense is not only possible in response of an ongoing armed attack. It can also be conducted facing an imminent attack (evidenced by hostile actions like preparatory cyber operations that will result in effects on the armed attack level) with no other reasonable hope of fending it off than responding immediately.[99]

Lawful Targets in a Cyber-Exchange

If the situation mounts to the point where forceful self-defense or retaliation becomes a lawful option, the question of how and what to attack arises. The cyber domain is characterized by pervasive dual-use infrastructure, which might be designated for civilian use but can by nature, location, purpose, or use be utilized for military purposes.[100] Thus, this infrastructure becomes a lawful military target under International Humanitarian Law (IHL), as the total or partial destruction, capture, or neutralization offers a direct and concrete military advantage. Ultimately this means that due to the heavy reliance on civilian products and infrastructure, the range of targetable objects in the cyber arena ex-

---

94 Schmitt, *Tallinn Manual on the International Law*, 54, Rule 13.

95 Carr, "Responsible Attribution," 7.

96 The International Court of Justice (ICJ) provided the precedence with the ruling on the Nicaragua case, in which it held the US responsible for breaches of International Humanitarian Law committed by a rebel group the US "effectively controlled." See Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 578.

97 The ICJ provided the precedence in the Corfu Channel case with the decision that a state violates its international obligations if it allows knowingly its territory to be used for unlawful acts against other states. See Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 578.

98 Goodman, "Cyber Deterrence," 108.

99 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 592.

100 This can be airspace management systems or communication lines that are partly used for military intentions.

pands, and systems with important civilian functions can legally be affected.[101] In the case of a forceful response in a cyber exchange, this brings certain flexibility in choosing targets but, at the same time, cyber means face the issue of difficult scalability and specific targeting. IHL requires that a weapon discriminates between combatants and civilians or civilian and military objects. If a cyber weapon cannot be directed at a specific military objective or generates uncontrollable effects, its employment is prohibited.[102] These restrictions do not apply for defensive measures and non-forceful means like malware that does not cause injury, damage, or loss of system functionality, even if it can spread into civilian systems.[103] If non-combatants that are not affiliated with an organized armed group and not under the control of a state are involved in a cyberattack, they can be targeted for the time they take direct part in the hostilities. In the cyber arena, this can start with gathering and spreading military intelligence by cyber means, probing an adversary's systems to identify vulnerabilities, or developing software specific to an attack.[104]

Application of Deterrence in the Cyber Domain

By considering the experiences made with the basic mechanisms of deterrence and by respecting the special implications and the legal characteristics of the cyber domain, it becomes clear that cyber deterrence cannot be applied in isolation but must be one vital component of a comprehensive security strategy.[105,106] In contrast to the nuclear concepts, defenses and resilience are a fundamental starting point to deny an adversary's success.[107] Besides *denial* by defense, the classical deterrence aspect of *retaliation* as threat of punishment plays a major role. As this research is based on a broader understanding of deterrence, two more ways come into focus: Deterrence by *entanglement* and by establishing *normative taboos*.[108]

Deterrence by Denial

Focusing on the defensive side becomes more important as the number of potential state adversaries with offensive cyber capabilities is on a steady rise.[109]

[101] Schmitt, "The Law of Cyber Targeting," 11.

[102] Inspite of this, if a cyber weapon is an alternative to a kinetic one and has a similar effect on the opponent, it ought to be preferred, as in most cases collateral damage is less likely, see Schmitt, "The Law of Cyber Targeting," 18.

[103] Schmitt, "The Law of Cyber Targeting," 16.

[104] Schmitt, "The Law of Cyber Targeting," 14.

[105] Nye, "Deterrence and Dissuasion in Cyberspace," 46.

[106] Cooper, "A New Framework for Cyber Deterrence," 105.

[107] Carberry, "Why There's no Silver Bullet for Cyber Deterrence."

[108] Nye, "Deterrence and Dissuasion in Cyberspace," 54.

[109] The Worldwide Threat Assessment of the US Intelligence Community shows a rise

Deterrence by denial aims to build resilience and the capacity to recover. Thereby, the adversary's benefits of an attack can be reduced until an engagement becomes futile and, after a blow, it can be ensured that cyber and non-cyber military responses are accessible for retaliation. There are measures of different sophistication and costs available,[110] but all have the common goal of chewing up the attacker's resources and time and disrupting his calculus of the perceived gain probability and value.[111,112] According to the "Assumed-Breach-Paradigm" there is no way of eliminating the successful penetration of one's networks. But the breech can be crafted difficult and tedious. Consequently, an attacker makes more "noise," needs more time, and becomes easier to identify as he leaves more traces.

On the way to a resilient culture, private-public-partnerships (PPP) and cyber insurances play a vital role. PPPs, on the one hand, bring together the government (as a legislator with rich resources in manpower, which is not focused on profit but effectiveness and can rely on intelligence services) with efficiency-driven privateers (who are highly experienced and technically specialized in the cyber domain, where they can access a large quantity of data and information).[113] On the other hand, mandatory cyber insurances for the economy contribute to systemic resilience and the denial of holding a nation's economy at risk. By putting a price tag on various private cyber practices, an incentive for higher standards and minding a "basic cyber hygiene" arises, whereby the low hanging fruits can be taken off the table and quick wins can be attained.[114] Furthermore, the reporting and connecting of attack-related data could be boosted significantly by profiting from the insuring industry's sophisticated crisis reaction

---

from probably three states in 2007 to over 30 states in 2017. See Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community" (Washington D.C.: Director of National Intelligence, February 2018), 6, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[110] An example for sophisticated and expensive measures is stockpiling redundant industrial power generators and transformers. Example for easy and cheap measures: Military training in celestial navigation in case of loss of global positioning systems. See Nye, "Deterrence and Dissuasion in Cyberspace," 56.

[111] Nye, "Deterrence and Dissuasion in Cyberspace," 56.

[112] Jasper, *Strategic Cyber Deterrence*, 111.

[113] The US government emphasizes this approach in its National Security Strategy: "In accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector so that we can better detect and attribute attacks." See *National Security Strategy of the United States of America* (Washington D.C.: The White House, 2017), 13, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[114] With relevant training to increase user awareness, up to 50 % of incidents could be avoided. See "ENISA Threat Landscape Report 2016" (Heraklion: European Union Agency for Network and Information Security, 2017), 81, www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

centers and processes.[115] Thus, the information asymmetry between privateers and government can finally be reduced, the reaction times can be increased, and the ground for a trust-based information sharing culture can be provided. To additionally foster private-public cooperation, "responsible disclosure agreements"[116] and "temporary clearances"[117] should be implemented.

Further starting points to improve the resilience and recovering capabilities can be found in the structure of the defense itself. It cannot be enough to protect only the outer perimeters of a system. As a breach is possible at any time, there are measures for an in-depth defense, able to detect the attacker inside the system, trace, identify, and disturb him. This can be supported by segmented networks and segmented sectors that do not allow, once a perpetrator is in, to spread his access over the entire system. Keeping vital capabilities as redundancies might be expensive at first glance but significantly lowers the gain probability of the adversary. Finally, protecting the supply chain is indispensable to avoid an opponent sneaking in. This requires an intense security-by-design debate with a consequent vetting of manufacturers and service providers and assessment which parts of critical supply chains need to be under national control.

Deterrence by denial is more than the mere repelling of a cyberattack. Conducted in a comprehensive manner, it can increase the time and survival factor, relive the force factor and provide the basis for the attribution factor on which retaliation becomes possible. If communicated in an appropriate way, the defense capabilities of a state can significantly influence the opponent's calculus of gain value and gain probability and give the government the leeway to pivot to major threats in the cyber arena.[118]

Deterrence by Retaliation

Responding to unwanted behavior with punishment is the most prominent way of deterrence. The goal is to promise to inflict costs on the attacker that outweigh the benefits anticipated from the initial attack.[119] This only works if the

[115] Umar Choudhry, *Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung* (Wiesbaden: Springer, 2014).

[116] Agreement between finder of vulnerabilities and software manufacturer to meet a publication deadline. The finder avoids the risk of being hold responsible for the exploitation of a vulnerability, the manufacturer receives appropriate time to analyze and fix the vulnerability and the user can rely on the fact that patches are not prolonged more than necessary. See *Die Lage der IT-Sicherheit in Deutschland 2017* (Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2017), 21, www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf.

[117] Temporally limited, case-related suspension of security clearances for a task-force to enable efficient information sharing amongst agencies and involved privateers.

[118] Nye, "Deterrence and Dissuasion in Cyberspace," 56.

[119] The US will "…impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities." See

attack can be attributed to an adversary in a sufficient way, addressing the three above-mentioned audiences.[120] Retaliation does not have to stay in the cyber domain but can take the shape of diplomatic, informational, military, and economic actions tailored to the opponent and considering potential back coupling effects due to international interdependencies.[121] Besides, geopolitical symmetry plays a key role. Retaliating against an adversary can mean to actuate an escalating series of retaliations outside the cyber arena, which in the long run can only be won if the escalation dominance lies on one's side.[122]

Countermeasures inside the cyber realm can be manifold and contain various levels of aggressiveness.[123] Outside the cyber domain, sanctions are the most common response to unwanted behavior, though in most cases they affect the population of a state more than the government. Therefore, it turns out to be more effective to invest resources in identifying attackers and aim sanctions on those individuals.[124] Even if no specific individual can be named, it is still possible to aim retaliation measures on relationships and social networks in which the attackers participate. This works, as all attackers are bound by dependencies and their calculus of gain and loss can be affected indirectly. Suspected groups can be cut from privileges like participating in the financial community and public outrage can be used to put internal pressure on the perpetrators and even outlaw them to the point where the network turns against them to avoid harm.[125]

Effective retaliation needs the time, force, survival, and attribution as baseline to contribute to the defense factor. Kinetic means have proved to be efficient tools of statecraft to respond to cyberattacks. As a result, conventional military means can be chosen as well as a nuclear answer in extremely severe cases.[126]

National Security Strategy of the United States of America, 13; Goodman, "Cyber Deterrence," 106.

[120] Nye, "Deterrence and Dissuasion in Cyberspace," 51.

[121] Jasper, *Strategic Cyber Deterrence*, 13.

[122] Goodman, "Cyber Deterrence," 109.

[123] As proposed in ascending order in Jasper, *Strategic Cyber Deterrence*, 177:

- Allow attackers to steal bogus files or embed beacons that reveal their location
- Bait files with malware to photograph the malicious actors using their webcam
- Infiltrate malicious actor networks to retrieve, alter or delete stolen data
- Implant malware to damage or ransomware to lock down actor computers
- Insert logic bombs into files before stolen to damage computers when opened
- Use DDoS attacks to interfere with malicious activity.

[124] President Obama did exactly this, by signing an Executive Order to block property and interests of people found to be meddling with the IT systems of the US's critical infrastructure. See Jasper, *Strategic Cyber Deterrence*, 97.

[125] Cooper, "A New Framework for Cyber Deterrence," 114.

[126] In the newly drafted nuclear strategy of the U.S., the possibility of nuclear retaliation for devastating cyberattacks is explicitly envisaged. See David E. Sanger and William J.

Deterrence by Entanglement

The modern international system is characterized by various dependencies, interconnections, and shared vulnerabilities. Deterrence by entanglement tries to encourage responsible state behavior by emphasizing the return from cooperation on mutual interests.[127] If an attack has negative back coupling effects on the attacker and benefits the status quo and its continuation, malicious engagement loses attractiveness. Entanglement boosts the survival and globalization factors and increases the adversary's perception of loss value and probability, even if the attack is not actively defended against or there is no fear of retaliation. The deterrence effect is contingent on a complex international deterrent relationship and works better when interdependencies are stronger.[128]

To enhance the effects of entanglement, confidence-building measures are an appropriate tool to strengthen international peace and security by increasing interstate cooperation, transparency, predictability, and stability.[129] In the cyber arena, communication hotlines, regional communication centers, prenotification agreements, and agreements on not attacking specific targets are feasible options and can be supplemented by forensic assistance in an IT incident and noninterference agreements with the workings of computer emergency response teams. Only establishing a cyber arms control regime faces some difficulties. Most technologies that could be described as cyber weapons are dual-use (like vulnerability assessment programs that can either find security gaps to protect a system or to exploit it) and, as a result, there is no consensus on what a cyber-weapon really is.[130] Above that, verifying the stock of cyber arms is nearly impossible, as this weaponry is not tangible and can easily be hidden or recreated after deletion.[131] To tackle this issue, "effects" instead of "used weapons" must be addressed.[132] In addition, normative taboos can be established, which is the last of the four ways of cyber deterrence.

Deterrence by Normative Taboos

With established strong norms, an aggressive actor will suffer reputational costs that will damage its soft power beyond the value gained from the attack. If a

---

Broad, "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *The New York Times*, January 16, 2018, www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html.

[127] Jasper, *Strategic Cyber Deterrence*, 16.

[128] China, which takes the legitimacy of its ruling party out of economic growth and thus depends on the internet, is far more entangled with the western world than the rather isolated North Korea. See Nye, "Deterrence and Dissuasion in Cyberspace," 58.

[129] Jasper, *Strategic Cyber Deterrence*, 150.

[130] Jasper, *Strategic Cyber Deterrence*, 16.

[131] Nye, "Deterrence and Dissuasion in Cyberspace," 60.

[132] Goodman, "Cyber Deterrence," 116.

state breaks a taboo (e.g., using nuclear weapons in a minor conflict against a weaker state), it faces the danger of being ostracized by the international system. This deterrence effect works although there is no active defense or a credible retaliation, but needs a certain degree of attribution. In history, the international community agreed on several implicit and explicit norms, such as the prohibition of chemical and biological weapons in the Geneva Convention.[133]

In the cyber domain, the normative agreement on the applicability of international law and the United Nations Charter was the first important step. In 2013, the UN's "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" proposed basic norms, like meeting the international obligations if a wrongful act gets attributed to a state, not to use proxies and not to tolerate non-state actors using a state's territory to commit wrongful acts.[134] Also, the use of International Tribunals and the International Criminal Court for the conviction of cybercriminals, terrorists, and state actors can be a powerful norm to deter and transmit a warning message.[135] Cyber-related norms can guide state behavior and increase predictability, trust, and stability in cyberspace as well as reduce the potential for conflict due to misperceptions. This only works, if norms are accepted by the majority of states and become institutionalized over time, e.g., under the umbrella of the UN.[136] Normative taboos can contribute to a certain extent to control over cyber weapons, even if it is impossible to establish a cyber arms control regime. They need to focus on tabooed effects and targets and, thus, can help distinguish which behavior is tolerated and which is ostracized.[137]

Conclusion

It became apparent that basic mechanisms of deterrence work in all realms, also in the cyber domain. Especially, as nuclear deterrence loses relevance in IR and current conflicts are ever more characterized by cyber components, the need for a comprehensive understanding of cyber deterrence is undeniable. Moreover, it was shown that five underlying factors (time, forces, survival, globalization, defense) of a game-changing new technology like the atomic bomb can be adapted to the cyber age. Above that, attribution plays a crucial role in the cyber domain and needs to be added to the discussion. It became clear that the international system is still in an early stage of applying IL in the cyber domain and that legislation must go a long way to catch up with the technological developments.

---

[133] Although this taboo did not stop Bashar al-Assad from using chemical weapons against his population, the international reaction (dismantling of Syrian chemical weapons in 2014 and the US led retaliation attacks of 2018) reflected the increased costs for breaking a normative taboo. See Nye, "Deterrence and Dissuasion in Cyberspace," 60.

[134] Jasper, *Strategic Cyber Deterrence*, 17.

[135] Quinlan, "Deterrence and Deterrability," 8.

[136] Jasper, *Strategic Cyber Deterrence*, 145.

[137] Nye, "Deterrence and Dissuasion in Cyberspace," 60.

The derived four ways to apply deterrence in the cyber domain (denial, retaliation, entanglement, and normative taboos) provide a feasible approach to integrating cyber deterrence aspects into a state's cybersecurity strategy (knowing that cyber deterrence can be only one pillar of an overall security strategy). However, those ways never work in an isolated way but rather in a comprehensive package with variable weighting of the single elements.[138] By complying with the basic mechanisms of deterrence and by tailoring the package to specific threat actors, a versatile and sound deterrence becomes possible.

Therefore, the hypothesis of this work can be validated: *Even in the cyber age, deterrence can be a powerful tool of statecraft and contribute to the protection of a state's national security interests!*

Still, effective deterrence does not arise by itself. It needs to be managed strategically or its effects will not be controllable. Politicians and strategists all around the world must prepare for a new and demanding age of deterrence to avoid sleepwalking into a real cyberwar.

In a subsequent article, the present findings will be applied in the example of Germany. It will be explained how Germany as an important player in an ever more digitized international system, can approach a cyber deterrence strategy to bolster its national security interests.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

Acknowledgment

Connections: The Quarterly Journal, Vol. 18, 2019 is supported by the United States government.

About the Author

Manuel Fischer is a security professional, working in the German defense sector with focus on counter-UAS Solutions. He looks back on twelve years of service in the German military (Bundeswehr) as a military police officer. During this time he acquired a Master of Science in Economics and Organizational Science from the University of the Federal Armed Forces in Munich. His service in the military was followed by his studies at the George C. Marshall European Center for Security Studies where he graduated its Master's program of International Security Studies concentrating on cyber security.
E-mail: fischermanuel@web.de.

[138] E.g., against the rather isolated North Korea, entanglement cannot be a major part of the set of the strategy, whereas against the powerful Russia, entanglement plays a far bigger role than retaliation.