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

Mika Kerttunen, *Connections QJ* 18, no. 1-2 (2019): 61-68
https://doi.org/10.11610/Connections.18.1-2.04

Research Article

Beyond Punishment: Deterrence in the Digital Realm

Mika Kerttunen

Cyber Policy Institute, Tartu, Estonia, https://cpi.ee/

Abstract: Deterrence theory has since its inception justified the build-up and maintenance of weapons arsenals assumingly guaranteeing our survival. However, we do not know whether deterrence theory works in practice: major wars may have been avoided for many other reasons than fear of punishment or (other) high costs. Skepticism towards cyber deterrence is used to justify unilateral, punitive, even preventive, pre-emptive, or continuous action against assumed adversaries. Nuclear weapons-centric deterrence, stressing the avoidance of reckless state behavior, could be improved to face the contemporary, technology-infused realities, where zero-tolerance of error or incidents, vital in the nuclear realm, is not realistic. As a result, we have come to accept or denounce cyber operations based on their targets and effects. As a contribution to achieving responsible state behavior in cyberspace, the author suggests utilizing cost calculation, the underlying assumption of deterrence theory, to the fullest: to include the promise of rewards in our policy options.

Keywords: cybersecurity, deterrence, cyber domain, compliance, tolerance, attribution.

The Comfortable Laziness of Deterrence Theory

Can anything new and meaningful be said of deterrence? Not necessarily starting from Hermocrates of Syracuse, any analysis of deterrence has at least to notice that deterrence, narrowly understood, refers to a threat of punishment.[1] At the

[1] Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960/1980); also Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966/2008); and Paul K. Davis, "Deterrence, Influence, Cyber Attack,

same, it should be noted that a wider reading acknowledges two aspects of deterrence: punishment and denial. Moreover, it is appropriate to table the latest interpretation, specially tailored for cyber affairs, which adds in the aspects of entanglement and normative taboos.[2]

Intellectual analysis starts with references to the logic of deterrence. Firstly, that at the core lies the pure assumed logic, or law, of economics. A rational actor is a calculative creation who knows what to choose: a lower cost (Formula 1).

Cost of compliance < *Cost of non-compliance*

Formula 1. The pure economic logic of being deterred.
(author's compilation)

Regardless of what is assumed to cause the deterring effect—abstaining from thought behavior: pain, failure, rewards, accumulation of costs, or shame—the theory, or the theories, assumes the adversary being belligerent, but, despite that, to act rationally, basing his or her decision-making on calculation, weighing the totality of potential while considering the likely costs and gains.[3] Secondly, it does not hurt to mention Schelling's fundamental thesis of the bargaining power of *harm versus no harm*:

> But suffering requires a victim that can feel pain or has something to lose. To inflict suffering gains nothing and saves nothing directly; it can only make people behave to avoid it. The only purpose ... must be to influence somebody's behavior, to coerce his decision or choice. To be coercive, violence has to be anticipated. And it has to be avoidable by accommodation. The power to hurt is bargaining power. To exploit it is diplomacy – vicious diplomacy, but diplomacy.[4]

Finally, one has to acknowledge the limitations of deterrence. Deterrence theory—and most importantly, its credibility—assumes resemblance between the imposed threats, the values of the adversary, and the anticipated rational behavior. Deterrence, as a principal political commitment, is absolute, yet real-life choices and the operationalization of deterrence call for challenging value

and Cyber War," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. For Hermocrates of Syracuse, see Thucydides, trans. Martin Hammond, *The Peloponnesian War* (Oxford: Oxford University Press, 2009).

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

3 Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).

4 Schelling, *Arms and Influence*, 2.

choices.[5] How much, for example, harm, cost, or pain is needed, and what constitutes cost, pain, or shame?

And how does the Other know of our capacity and of the calculations we have taken on his/her behalf? Communication is imperfect, and perfect understanding impossible. Moreover, there is an asymmetry of information. For example, while it is safe to assume that the attacker has fairly sufficient knowledge of the targeted cyber system and the values associated with it, the defender is not necessarily aware of the attacker's identity or strategy or payoffs. Moreover, the cyber defender may be forced to act only at certain points in time, while the cyber attacker is free to become active at any time. This is emblematic of the dilemma between *discrete time* for one player and *continuous time* for the other.[6]

Regarding cyberspace, it is appropriate to notice that deterrence in cyberspace is challenging or does not function at all. The very fact of malicious cyber operations taking place is hard to establish. Further evidence comes from the stealthy, speedy, or non-attributable nature of cyber activities, which often are conducted by non-state actors, or that there are no appropriate means or political-legal frameworks to punish the cyber-perpetrators.

In fact, the very claim that deterrence functions cannot be verified or falsified. The very deterring effect is a cognitive one. Deterrence theory, albeit often loaded with calculations, cannot explain or predict any behavior; at best, it is *an ideal or hypothetical set of facts, principles, or circumstance,* or simply, *an abstract thought*.[7]

Accordingly, the study of deterrence has become studies of certain elements considered to be essential in the established canon of deterrence. Moreover, skepticism towards cyber deterrence is used to justify unilateral, punitive, even preventive, pre-emptive, or continuous action: since deterrence does not work in cyberspace, it is responsible for taking action and causing costly effects to the alleged Other, especially as there is no threat of annihilation by retaliation. This

---

[5] Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND, 2017), 21–22, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf; Andrew Higgins, "Two Border Cities Share Russian History – and a Sharp European Divide," *The New York Times*, November 9, 2017, https://www.nytimes.com/2017/11/09/world/europe/narva-estonia-ivangorod-russia.html.

[6] Kien C. Nguyen, Tansu Alpcan, and Tamer Basar, "Security Games with Incomplete Information," in *Proceedings of the 2009 IEEE International Conference on Communications*, 14-18 June 2009, Dresden, Germany, https://doi.org/10.1109/ICC.2009.5199443 (studying the game theory of security games and discrete time); Stefan Rass, Sandra König, and Stefan Schauer, "Defending Against Advanced Persistent Threats Using Game-Theory," *PLoS ONE* 12, no. 1 (2017), https://doi.org/10.1371/journal.pone.0168675.

[7] *Merriam-Webster English Dictionary.*

belief is based on a limited understanding of cyber deterrence. Despite its narrow, formal correctness, it is dangerously wrong.[8]

We simply do not know if deterrence actually works or not. This uncertainty, together with the fact, claim, or assumption that with the cyber condition we have entered at least partially a new operating environment, calls for a new narrative of deterrence.

A New Narrative of Deterrence: Four Claims

Changed Context

Although the logic of deterrence could be traced to general and ancient human behavior, the genealogy of deterrence theory is conditioned by the bipolar Cold War. Then the double-intent of the two superpowers can be said to have sufficient power to destroy the other while ensuring the survival of human life on the planet. The concept of deterrence allowed to justify the former and to assure of the latter.

Nuclear weapons and the superpower ability to destroy the planet has not disappeared. Yet, the conditions and the context of cyber deterrence are different. Whereas previously deterrence stressed the avoidance of reckless state behavior, the contemporary cyber discourse focuses on responsible state behavior. Deterrence, as we have come to know it, does not seem appropriate or credible.

Wider Tolerance

Moreover, whether in the nuclear setting, in the Cold War and now, the culture of zero tolerance prevailed. Failures of deterrence, at least in the purest sense, would have been unacceptable. A nuclear or any major military attack would have been met by countermoves, even retaliation, when everything had already been lost.

In cyber affairs, nobody could live with zero tolerance. Information and communications systems are inherently vulnerable, prone to technical incidents or human errors, let alone deliberate attacks. In fact, if during the Cold War superpower military confrontation was acceptable in the global periphery—Asia, Africa, and Latin America—we have now come to have three *de facto* layers of acceptance of cyber operations.

Readily accepted are operations conducted by intelligence agencies, security and law enforcement organs and armed forces against universally recognized extremist, terrorist or criminal organizations since, fo example, the United Nations Security Council (UNSC) Resolution 1373 (2001) determines all forms of ter-

[8] Similarly wrong is to uncritically assume that cyber activities are invisible, fast and non-attributable. Any analysis beyond airport literature can notice the tangible effects and the months and years of preparation of cyber-attacks, and the official attributions made to state and non-state actors. The speed of light, as well as the speed of a bullet or a fighter plane, are very poor indicators to inform of the speed of an attack, operation or campaign.

rorism as constituting a threat to international peace and security. Therefore, it is relatively easy for the international community to accept, even hail, the US offensive military cyber operations against the "Islamic State." On the other hand, state cyber operations within existing dyadic conflicts or against lower value targets, hypocritical or not, are contingently accepted. For example, Israeli cyber operations against the Syrian government, or Hezbollah, do not trigger international objections beyond the usual – but the US ones against the very same targets would. The alleged Dutch intelligence agency operation infiltrating to Moscow State University systems[9] did not make any waves, maybe because states are reluctant to problematize intelligence activities they all are conducting, and maybe because the target of the operation was (said to be) a Russian origin cyber-criminal grouping. Operations which seem to be unacceptable are ones that properly jeopardize the international order or national security. Therefore, operations such as the 2016 infiltration into the Democratic National Congress servers and exfiltration of data or the 2017 attempt to hack the Organisation for the Prohibition of Chemical Weapons are considered dangerous and irresponsible, receiving wide international condemnation.

Obviously, this factual tolerance of cyber operations challenges the established logic of deterrence: they are incompatible. The very absence of any serious cyber operation rather witnesses either of states' inability or their caution to conduct such effect-creating and profound operations in peacetime than of deterrence. Yet, the practice of cyber operations by exploiting the thresholds of use of force and armed attack challenge international law and, most seriously, the rule of law many of the keen operations verbally are endorsing.

More Approaches

Conceptually, and borrowing from ancient Chinese thinking, deterrence by punishment is a negative approach and deterrence by denial – a neutral one. As we are being told, the former seeks actively to reduce the bad actor's values, and the latter denies any increase in those values. If the rational man's calculative logic is correct, as it is assumed, then offering rewards should also deter an actor from taking action he would otherwise take – positive deterrence: deterrence by benefits.

Such benefits can be created in several ways. Mirroring the concept of deterrence by punishment, deterrence by benefits could reward certain behavior of states. Taking into account the concept of deterrence by denial, it could feature the development of infrastructure, cooperation models, exchange of know-how, or the setting of plurilateral, sub-regional, or other common goals that leverage the economic and social benefits of information and communication technologies. Benefits can also be achieved, in the context of entanglement, as a result

[9] Rick Noack, "The Dutch Were a Secret U.S. Ally in War against Russian Hackers, Local Media Reveal," *The Washington Post*, January 26, 2018, www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/.

of reduced expenditure and optimization of costs by way of joint reduction of cyber risk. Furthermore, the anticipated benefits could be improved reputation, ranking in relevant international venues or assessments, or acknowledged leadership in international processes. Compared to the normative taboo and the zero-tolerance tools, deterrence by benefits would emphasize maximizing common benefits and therefore full support and universal acceptance/endorsement of certain behavior.

It is further hypothesized that the classical theory of deterrence no longer satisfies states' political ambitions sufficiently. Especially in Europe, there is a strong hesitation towards hard-security deterrents, including sanctions and countermeasures imposed under, and especially in the outskirts of international law. Instead, states are increasingly interested in economic and social incentives behind the behavior of their counterparts.

A key criticism towards deterrence by punishment is the fact that wherever punishment becomes actionable, deterrence has, by definition, failed. Accordingly, in the case of benefits, the anticipatory and preventive nature of deterrence is maximized. It can also be argued that deterrence by benefits maximizes reciprocity and, therefore, promises the widest possible platform of shared interests and universal acceptance of certain behavioral modalities. By enhancing the study of changing the calculus of malicious or hostile acts, states could increase the return of security investments. It is presumed that a reduced margin of politico-military risk also lowers forced defense and military expenditure while adding to the social and economic budget that creates resilience and strengthens the information society.

Investments into resilience and good security practices, in turn, are likely to significantly increase the cost of bad behavior, therefore creating additional denial thresholds. In this context, resilience as an actor-neutral measure is emphasized and promoted.

Nuanced Tools

States or groups of states should thus look beyond sanctions, or the negative aspects more generally. Indeed, we should recognize how well resilience as implicit deterrence by denial works: the number of effect-creating cyber operations is very small, especially compared to cybercrime and common talk of cyberwar being waged.[10] Actually, the very extent of cybercrime testifies of the insufficient governmental and organization investments in the capacity needed to deny cybercriminals from achieving their objectives. Moreover, national and international cybersecurity policies should incorporate positive agendas with rewards.

[10] Eneken Tikk, Kristine Hovhannisyan, Mika Kerttunen, and Mirva Salminen, *Cyber Conflict Fact Book: Effect-Creating State-on-State Cyber Operations* (Jyväskylä: Cyber Policy Institute, 2019). This analysis is based on the publicly known state cyber operations the Council of Foreign Relations "Cyber Operations Tracker" and other databases had gathered.

Conclusion

As we have come to know, deterrence is a cumbersome and inappropriate tool to understand the cyber realm. The conditions of the cyber condition and the new genealogy of deterrence are different from and far more nuanced than those of the nuclear setting.

As technological, political, and societal parameters and premises are different; therefore, the conclusion is too. Cyber deterrence to function as a cybernetic steering mechanism of state behavior needs paradoxically be built on the acceptance of error and incidents as well as low-intensity attacks. This acceptance draws lines between tolerable and intolerable. We, the West, have to ensure that the standards of responsible state behavior become as high as possible. Our eagerness to exploit our technological supremacy and conduct cyber operations should not undermine the rule of law and higher moral ground. Since deterring an actor is both theoretically questionable and, in the cyber realm, practically not feasible, sanctions of all kinds are to create state practice and boundaries of responsible/irresponsible state behavior.

Managing the new setting of uncertainty, blurred lines of responsibility, the many thresholds, and the many actors cannot solely rely on the black-or-white logic of the negative, i.e. punishment. Resilience should replace punishment and caution brinkmanship in our strategic lexicon. Robust (national) resilience as threat-neutral and de-escalatory is also better suited to accommodate unpredictability, a feature particularly relevant to the cyber context, than deterrence, or persistent engagement for that matter. The success of the dominating risk and threat (actor) based approaches, or both deterrence and persistent engagement, being conditioned by the accuracy of the (pre-) assessments is in itself too risky.[11] The West has to incentivize responsible behavior in cyberspace. Resilience and rewards coupled together create a powerful and peaceful policy option no other state or group of state can offer. The negative alone is insufficient.

Thus, in the new formula (Formula 2 below) of being deterred the law of economics still rules, but costs are replaced by rewards.

[11] Gerard de Vries, Imrat Verhoeven, and Martin Boeckhout, "Governing a Vulnerable Society: Toward a Precaution-Based Approach," in *Vulnerability in Technological Cultures: New Directions in Research and Governance*, ed. Anique Hommels, Jessica Mesman, and Wiebe E. Bijker (Cambridge, MA: MIT Press, 2014), 225. The referred chapter is based on the report *Uncertain Safety* which the Dutch Scientific Council for Government Policy (WRR) has adopted as official advice to the Dutch cabinet. Risk management adopted, or at least cited, in many national cybersecurity strategies, seeks to identify and evaluate risks in terms of probabilities and extent of damage and design and take measures to limit or control those risks considered unacceptable.

Rewards of compliance > Rewards of non-compliance

Formula 2. The new economic logic of being deterred.
(Author's compilation)

This turn does not assume the almost automatic bellicosity of the Other. We thus avoid the illusion of deterring the Other in a situation where such bellicosity is not necessarily being considered taking. Instead, we focus on the more likely motivation and ambitions governments have – positive rewards. Obviously, a leader determined to go to war will not be turned away by threat of punishments, anticipated hardships, or benevolent rewards.

Such a turn in thinking would not be appreciated by the security – cyber-industrial complex riding on the threat and promise of an apocalyptic future. For the rest of the humankind preferring peace, prosperity and global justice such turn would make sense.

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

LTC (ret., Finish Army) Mika **Kerttunen**, D.Soc.Sc. (Pol.), is Director of Studies, Cyber Policy Institute (Tartu, Estonia). He is a graduate of the Finnish Military Academy and General Staff Officer Course as well as the Royal Norwegian Command and Staff College. Kerttunen studied world politics at the University of Helsinki and analysed in his 2009 dissertation Indian foreign and nuclear policy. After his military service he has been focusing on cyber issues in foreign and security policy, the development of cyber norms, and the development of national cyber security strategies and military cyber doctrines. Dr Kerttunen is advisor at the Finnish delegation at the UN Group of Governmental Experts on Information Security (2016-2017) and Visiting Faculty Member at the University of Tartu Law School.