# Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity

Mieke Eoyang* & Chimène Keitner**

As we move toward a world of fully connected devices that share data on an unprecedented scale (the "Internet of Things" or IoT), the cybercrime enforcement gap will pose an ever-greater threat to personal and national security.[1] A variety of factors contribute to the relative vulnerability of the United States to harm from malicious cyber activity (MCA).[2] In 2018, then-DHS Secretary Kirstjen Nielsen warned that "our digital lives are in danger like never before."[3] She identified the threat as coming from "hostile states, terrorists, and transnational criminals"—and, one might add, domestic terrorists and criminals.[4] In the face of these various threats, U.S. government responses to national security challenges in both the physical and virtual worlds have increasingly blurred the line between transnational crime and armed conflict. This shift in narrative comes at a cost. The displacement of law enforcement approaches by an armed conflict model carries implications for institutional design, legal authorities, and resource allocation. Notably, one result of a militarized approach to transnational cyber threats has been to leave domestic law enforcement officers inadequately trained, inadequately resourced, and inadequately supported to identify, deter, and punish offenders.[5] The urgent need for better resourced and better coordinated law enforcement responses suggests a corresponding need to keep the essentially criminal nature of most malicious cyber activity in focus, even as we grapple with the implications of MCA that is conducted, sponsored, encouraged, or tacitly permitted by nation-states.

This contribution aims to encourage greater self-awareness about the consequences of viewing MCA predominantly through the lens of armed conflict, rather than law

---

* Then-Vice President for the Third Way National Security Program and Chairperson of the Cyber Enforcement Initiative. This article was completed before her return to government service, and represents her personal views, and not those of the US government, the Department of Defense, or President Biden. 

** Alfred & Hanna Fromm Professor of International and Comparative Law, UC Hastings Law.

1. *See, e.g.*, Allison Peters & Amy Jordan, *Countering the Cyber Enforcement Gap: Strengthening Global Capacity in Cybercrime*, 10 J. NAT'L. SECURITY L. & POL'Y 487 (2020).

2. *See* Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations*, AEGIS SERIES PAPER NO. 1806 (2018), https://perma.cc/M8LJ-HQZM.

3. DEP'T OF HOMELAND SECURITY, SECRETARY KIRSTJEN M. NIELSEN REMARKS: RETHINKING HOMELAND SECURITY IN AN AGE OF DISRUPTION (Sept. 5, 2018), https://perma.cc/DU2F-KXML.

4. *See also* FBI Director Christopher Wray, Statement Before the Senate Homeland Security and Governmental Affairs Committee (Oct. 10, 2018) (indicating that "[v]irtually every national and criminal threat the FBI faces is cyber-based or technologically facilitated"), https://perma.cc/DNU6-SUC5.

5. *See, e.g.*, Nick Selby, *Local Police Don't Go After Most Cybercriminals. We Need Better Training.*, WASH. POST (Apr. 21, 2017, 6:00 AM), https://perma.cc/6P9G-4LL8; on the scale of the problem, *see e.g.*, JONATHAN LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME (2018).

enforcement. The tension between competing paradigms for addressing criminal activity that rises to the level of a national security threat is familiar from—and can trace its roots to—the U.S. response to the attacks of 9/11. Rather than deal with transnational terrorism primarily as a law enforcement matter, the United States opted for a military response, invading Afghanistan in 2001 and Iraq in 2003. In the wake of 9/11, the U.S. government adopted the term "Global War on Terror" or GWOT and began viewing measures taken against terrorist groups and nation-states that harbor or support them through an armed conflict, rather than a law enforcement, lens. Many policy decisions previously addressed through civilian authorities and processes were revisited under new national security authorizations as part of this global "war." For example, the decision to prosecute "enemy combatants" using military commissions rather than Article III courts exemplifies the view that the United States was, and is, engaged in a "war" on terror. Early justifications for the Bush administration's Terrorist Surveillance Program, later revealed as "Stellar Wind," rested on the President's national security powers, and ignored existing civil and law enforcement authorities under the Foreign Intelligence Surveillance Act of 1978 (FISA).[6] This militarized paradigm has become embedded in our vocabulary, and it has informed the allocation of authority and resources in efforts to protect the United States from terrorist threats.

This contribution seeks to identify and assess the frameworks used to describe and deter malicious cyber activity, and to highlight legal and operational challenges in tackling problems that arise where these frameworks overlap or intersect. To that end, we examine two different models, an "armed conflict model" and a "law enforcement model," that have been used to address the threat posed by such activity. The terms cyber*war* and cyber*crime*, respectively, encapsulate each of these models—yet the line separating these categories is not well defined, and both terms have been used by laypersons and experts alike to describe conduct ranging from network intrusions to data exfiltration to denials-of-service. Our analysis of these ambiguities and their implications proceeds in four parts. Part I canvasses recent U.S. government approaches to combating MCA. Part II explores the assumptions underlying the predominant armed conflict model. Part III discusses the implications of characterizing MCA as cyberwar as opposed to cybercrime. Part IV concludes by suggesting that these characterizations should be viewed along a continuum, and that the law enforcement model should not be given short shrift by policy makers or—perhaps most importantly—appropriators.

## I. U.S. GOVERNMENT RESPONSES TO CYBER THREATS

As the United States began grappling seriously with cybersecurity and malicious cyber activity, it did so within a militarized lens. In 2009, the Secretary of Defense directed the establishment of Cyber Command within the Department of

6. *See* U.S. DEP'T JUST., OFF. INSPECTOR GEN., OVERSIGHT & REV. DIV., REPORT NO. 2009-0013-AS, REV. DEP'T JUST.'S INVOLVEMENT WITH PRESIDENT'S SURVEILLANCE PROGRAM (U) (2009), https://perma.cc/P7H9-384M.

Defense.[7] That same year, an international group of experts began deliberations on what became known as the Tallinn Manual, an attempt to detail the applicability of international law principles to cyber conflict.[8] A second Tallinn Manual 2.0 elucidated international legal principles applicable to peacetime cyber operations.[9] Unfortunately, experts were unable to agree on how to define the dividing line between cyber operations that amount to armed attacks and those that fall short of this level, which might also help differentiate between situations that warrant an armed conflict approach and those that should be treated as law enforcement matters.[10]

The lack of clarity about what amounts to an armed attack in cyberspace also makes it difficult to disentangle and de-conflict militarized and civilian approaches to malicious cyber activity. Within a cyberwar frame, the Department of Defense has inaugurated a policy of "defend[ing] forward" to "disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[11] On the law enforcement side, the Department of Justice has pursued a cybercrime strategy of "attribution by indictment" to identify, deter, and punish malicious cyber actors who target the private sector, even when they do so on behalf of nation-states.[12] Although, as explored below, some nation-state-sponsored cyber activity challenges the idea that we can always draw a clear distinction between transnational cybercrime and malicious activity just below the armed attack threshold, privileging a war (or potential war) model over a crime model carries substantial implications for the domestic allocation of resources and authority, and for the prospects of international cooperation to deter would-be cyber criminals and enforce prohibitions on MCA.[13]

We readily acknowledge that placing greater emphasis on the law enforcement paradigm is not a panacea. Notably—perhaps more so than any other previous

7. SEC. OF DEF., ESTABLISHMENT OF A SUBORDINATE UNIFIED U.S. CYBER COMMAND UNDER U.S. STRATEGIC COMMAND FOR MILITARY CYBERSPACE OPERATIONS (2009), https://perma.cc/G37D-YXVB.

8. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed. 2013).

9. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt, ed. 2017).

10. *See* Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical* Vade Mecum, 8 HARV. NAT. SEC. J. 239, 245 (2017) (indicating that "[a]lthough the International Group of Experts agreed that cyber operations resulting in physical damage or injury are unambiguously uses of force, no consensus could be reached as to when cyber operations not having those consequences qualify").

11. U.S. DEP'T DEF., SUMMARY: DEP'T DEF. CYBER STRATEGY 1 (2018), https://perma.cc/JK94-SMT4.

12. *See* Chimène I. Keitner, *Attribution by Indictment*, 113 AJIL UNBOUND 207 (2019) (identifying and analyzing the novel practice of publicly linking MCA to foreign states by announcing and releasing detailed indictments against foreign actors for violating U.S. criminal law); *see also* Garrett Hinck & Tim Maurer, *Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity*, 10 J. NAT. SECURITY L. & POL'Y 525 (2020) (further exploring this practice).

13. These implications were highlighted by President Obama's use of the term "cyber-vandalism" to characterize North Korea's hack of Sony Pictures Entertainment. For criticism of this approach, see, e.g., David Rothkopf, *Obama Is Wrong: The Sony Hack Is Not "Cybervandalism"*, FOREIGN POL'Y (Dec. 22, 2014), https://perma.cc/ZLF9-MU6M.

form of criminality—cyber criminality almost invariably involves actions (whether human or machine) across multiple territorial jurisdictions, potentially implicating multiple different domestic legal systems, and even different definitions of what constitutes criminal behavior. Even under a law enforcement model, the degree of international cooperation required to apprehend and punish cyber criminals has, to date, proved to be a major obstacle to creating effective deterrence, even when the authors of MCA can be identified and their involvement proven with a sufficient degree of certainty based on admissible evidence.[14] Moreover, the potential involvement of nation-state actors means that the foreign policy consequences of law enforcement decisions need to be assessed on a regular basis.[15] In addition, in certain circumstances and with respect to certain actors, an armed conflict model might be more appropriate.[16] The need for flexibility and coordination requires an institutional structure that can oversee, direct, and deconflict enforcement initiatives.[17]

With this backdrop in mind, this contribution aims to provoke deeper thinking about the relationship between the armed conflict model and the law enforcement model in addressing pervasive, costly, and disruptive MCA engaged in by a range of actors.[18] In particular, it seeks to focus attention on a neglected aspect of contemporary approaches to deterring and punishing MCA, as illustrated in the diagram below. Just as there are both machine-based and human-based defensive responses to MCA, so too are there machine-based and human-based offensive responses. In our view, human-based offensive responses have been insufficiently resourced and developed.

---

14. *See, e.g.*, Mike Eckel, *For Russia and U.S., Uneasy Cooperation on Cybercrime Is Now a Mess*, RADIO FREE EUR/RADIO LIBERTY (Apr. 29, 2017), https://perma.cc/529D-C8XW; Ron Cheng, *Prospects for U.S.-China Cybercrime Cooperation: The Road Thus Far*, LAWFARE (Mar. 9, 2017), https://perma.cc/9KZV-EPW6.

15. It is curious in this regard that there was no apparent State Department representation in the bipartisan Cyberspace Solarium Commission formed to study these issues. *See* Sen. Angus King & Rep. Mike Gallagher, *Announcing the Cyberspace Solarium Commission*, LAWFARE (Aug. 19, 2019, 3:13 PM), https://perma.cc/RGZ3-KS5G.

16. There is also a connection between state-sponsored and state-executed cybercrime and a state's ability to conduct armed attacks. *See, e.g.*, Sébastien Seibt, *How Cybercrime Funds North Korea's Nuclear Programme*, FRANCE24 (Aug. 8, 2019, 15:14), https://perma.cc/7CQ7-TVE9.

17. Although this institutional framework could take various forms, it did not escape notice that the White House eliminated the position of cybersecurity coordinator on the National Security Council in May 2018. *See* Nicole Perlroth & David E. Sanger, *White House Eliminates Cybersecurity Coordinator Role*, N.Y. TIMES (May 15, 2018), https://perma.cc/4TBR-XGFR.

18. We have, for the purposes of this paper omitted, analysis of cyber attacks under other legal frameworks designed to regulate spaces outside of designated sovereignty of a particular nation-state such as treaties relating to outer space law, the moon, and Antarctica. Those domains, unlike cyber, are not easily accessed or regularly used by civilian actors. Further, we have not analyzed responses to MCA under two other legal frameworks designed to regulate international commons: those governing the use of international airspace and the law of the sea. Analyses that draw on these paradigms generally focus on how to *prescribe* rules for cyberspace, whereas we are concerned primarily with how to *enforce* prohibitions on criminal activity that already exist under various countries' domestic laws.

**Fig. 1**
**Typology of Responses to MCA**

| | **Defensive** | **Offensive** |
|---|---|---|
| **Machine** | Network security (technical) | "Defending forward"; network-to-network; persistent engagement |
| **Human** | Cybersecurity (behavioral) | *Criminal law responses*; government-to-individual |

Defensive capabilities at the "machine" level must continue to be developed and implemented, just as offensive machine capabilities—used appropriately—can play an important role in U.S. cyber strategy. Likewise, it is essential to cultivate defensive human capabilities through education and outreach (and, if necessary, incentives such as liability schemes). At the present time, however, our human offensive capabilities in the form of local, state, and federal law enforcement responses remain severely neglected. There are good reasons to make the development of such capabilities a priority.

We recognize that some of the above categories can more accurately be placed along a continuum, rather than in discrete boxes. Similarly, intelligence and counter-intelligence activities occupy an amorphous space between the traditional categories of war and crime. Appropriate responses to MCA cannot be identified solely on the identity of the perpetrator (e.g., nation-state vs. private actor) or the aim of the conduct (e.g., geopolitical vs. financial gain). Nation-state-sponsored activity can be directed towards both public and private sector activities (which can themselves be difficult to disentangle), and both state and non-state actors can have motives ranging from economic gain to geopolitical disruption (or both).[19]

In the absence of a comprehensive international legal framework governing MCA, most deterrence and enforcement activities remain rooted in domestic law, including domestic criminal law.[20] Importantly, as senior DHS officials have noted, "the vast majority of cyberspace is civilian space."[21] One might think these factors would contribute to a widespread understanding of MCA as

19. Jason Healey's work has been particularly helpful in thinking about the continuum along which nation-states conduct, support, and interdict MCA. *See* JASON HEALEY, ATLANTIC COUNCIL, BEYOND ATTRIBUTION: SEEKING NATIONAL RESPONSIBILITY FOR CYBER ATTACKS (Feb. 22, 2012), https://perma.cc/2BJN-GN5K.

20. That said, it is worth noting that sixty-three countries, including the United States, have ratified the Budapest Convention on Cybercrime. Budapest Convention on Cybercrime, Nov. 23, 2001, ETS No. 185. In addition, at the time of writing, two groups were being formed under UN auspices to continue the arduous process of elaborating norms of "responsible State behavior" in cyberspace: a sixth UN Group of Governmental Experts (to start in 2019 and report to the UN General Assembly in 2021 under the terms of its founding resolution, https://perma.cc/P6YB-3JBK, and a new open-ended group (to start in 2019, and report to the UN General Assembly in 2020 under the terms of its founding resolution, https://perma.cc/UEE6-JCGD).

21. Jane Holl Lute & Bruce McConnell, *Op-Ed: A Civil Perspective on Cybersecurity*, WIRED (Feb. 11, 2011, 7:00 AM), https://perma.cc/K297-8MY8.

predominantly a challenge for transnational law enforcement, analogous to combating other forms of transnational organized crime. Nonetheless, the terms commonly used to describe MCA come almost uniformly from a military lexicon. The pervasive use of these terms tends to reinforce the predominance of an armed conflict model for deterring, and defending against, non-militarized forms of MCA.[22]

Invoking a war frame may lead policymakers to undervalue malicious cyber activity aimed at civilian targets for financial gain. The FBI estimates that these forms of MCA—comprising internet-enabled theft, fraud, and exploitation—caused at least $2.7 billion in financial losses in 2018.[23] The Center for Strategic and International Studies assessed in 2018 that "cybercrime may now cost the world almost $600 billion, or 0.8% of global GDP."[24] In light of these trends, a more balanced approach to the problem of digital insecurity would place "more emphasis on law enforcement and diplomacy to prevent an overreliance on the military," which is ill-suited to addressing the full range of MCA engaged in by both state and non-state actors, as described further below.[25]

## II. ASSUMPTIONS UNDERLYING THE ARMED CONFLICT MODEL

Unauthorized cyber intrusions of all types are referred to colloquially as "cyberattacks." Although experts have parsed the threshold at which MCA amounts to an "attack" for the purposes of international humanitarian law,[26] the terms "cyberattack" and "cyberwar" have become short-hand in discussing all forms of MCA, without distinction. As a threshold matter, the Department of Defense views "cyberspace" as a war-fighting domain, along with air, land, sea, and space.[27] Within these domains, armed conflicts can take the form of international armed conflicts between nation-states (IACs), on the one hand, or non-international armed conflicts between governmental forces and non-state armed

22. Additional unintended consequences might include the exclusion of certain business losses from cyber insurance coverage. *See, e.g.*, Adam Satariano & Nicole Perlroth, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong.*, N.Y. TIMES (Apr. 15, 2019), https://perma.cc/SNV8-BGNY (describing insurance companies' refusal to pay claims for business losses associated with the NotPetya virus on the grounds that they fell under the "war exclusion").

23. FED. BUREAU INVESTIGATION, 2018 INTERNET CRIME REPORT 5 (2018), https://perma.cc/G3RU-VUPT.

24. CSIS, ECONOMIC IMPACT OF CYBERCRIME—NO SLOWING DOWN (Feb. 2018), https://perma.cc/H7A4-Y9GX.

25. *See* Mieke Eoyang, Allison Peters, Ishan Mehta & Brandon Gaskew, *To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors*, THIRD WAY 2 (Oct. 29, 2018) https://perma.cc/3HN9-52WB.

26. *See, e.g.*, Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT. SEC. L. BR. 33, 33 (2011); *see also* Kyle Genaro Phillips, *Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain*, 70 JOINT FORCE Q. 70, 72 (2013) (putting forth a diagram derived from Walker's analysis).

27. DEP'T DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA 3 (2018); *but cf.* Martin C. Libicki, *Cyberspace Is Not a Warfighting Domain*, 8 I/S: A J. OF L. & POL'Y 321 (2012) (identifying "conceptual errors that may arise by thinking of cyberspace as a warfighting domain analogous to the traditional warfighting domains").

groups within the boundaries of a single state (NIACs), on the other. More recently, "transnational" or "global" NIACs have challenged the dividing line between these categories.[28]

The contemporary idea that nation-states maintain a monopoly on the legitimate use of force within their respective territories, and that they are willing and able to control malicious activity emanating from their territories, breaks down when there are relatively few barriers to entry for engaging in that activity. This is particularly true when it comes to MCA. However, in discussing MCA within a war frame, a series of inferences are often made that lead analysts to posit that the deterrence frames from the armed conflict context can be applied directly to cybersecurity. Cyberwar, like "cyberspace," is "an influential and charismatic metaphor" which shapes the way that many scholars approach their analysis.[29] Indeed, throughout both the popular and academic literature, malicious cyber acts are frequently discussed in a war frame—whether those acts are performed to disrupt services, gather information, steal or extort money, or influence human behavior.[30] In the academic literature, adopting the war frame leads to analysis of cyber activity within existing paradigms designed to avert conflict, such as deterrence via threat of retaliation. This, in turn, can lead to concerns about escalation.

As James Miller and Neal Pollard have emphasized, "deterrence strategy should seek to influence a competitor's decision-making by denying it the gains

28. For literature on the challenges involved in classifying armed conflicts, see, for example, David E. Graham, *Defining Non-International Armed Conflict: A Historically Difficult Task*, 88 INT'L L. STUD. 43, 50–52 (2012) (noting that the U.S. rarely "officially" determines when a conflict has crossed the threshold between international and non-international conflict, and that it views the "basic provisions of the law of armed conflict" as applying to both categories as a policy matter of policy); Dapo Akande, *Classification of Armed Conflicts: Relevant Legal Concepts*, *in* ELIZABETH WILMSHURST (ed.), INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS, ch. 3 (2012) (examining the history and consequences of distinguishing between international and non-international armed conflicts); Andreas Paulus & Mindia Vashakmadze, *Asymmetrical War and the Notion of Armed Conflict: A Tentative Conceptualization*, 91 INT'L REV. OF THE RED CROSS 95 (2009) (emphasizing the need for objective criteria to determine when international humanitarian law applies in a given conflict).

29. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 16 (2008).

30. Titles invoking the armed conflict model include: JOHN P. CARLIN, DAWN OF THE CODE WAR: AMERICA'S BATTLE AGAINST RUSSIA, CHINA, AND THE RISING GLOBAL CYBER THREAT (2018); DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE (2018); P.W. SINGER & EMERSON T. BROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA (2018); FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBERWAR (reprint edn., 2017); RICHARD A. CLARKE & ROBERT K. KNAKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (2012). Titles that distinguish "cybercrime" from "cyberwarfare" include: JONATHAN LUSTHAUS, INDUSTRY OF ANONYMITY: INSIDE THE BUSINESS OF CYBERCRIME (2018); RICHARD A. WHITE, CYBERCRIME: THE MADNESS BEHIND THE METHODS (2018); IGOR BERNIK, CYBERCRIME AND CYBERWARFARE (2014); P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW (2014); BRIAN KREBS, SPAM NATION: THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR (2014). Titles that fall in-between include: MARC GOODMAN, FUTURE CRIMES: INSIDE THE DIGITAL UNDERGROUND AND THE BATTLE FOR OUR CONNECTED WORLD (reprint edn. 2016).

of its actions, irrespective of any retaliation or escalation."[31] As Jason Healey puts it, "[t]he debate on cyber conflict has gotten so locked into deterrence, escalation, coercion, and signaling we pundits often forget that conflict is sometimes straightforward and you just have to stop adversaries from punching you."[32] This insight has relevance in both the armed conflict and law enforcement paradigms, as illustrated by Israel's Iron Dome program.[33] Even traditional deterrence theory would acknowledge the important role of "deterrence through denial," in addition to "deterrence through punishment." In the words of Andrew Krepinevich, Jr., "[s]ince World War II, U.S. defense strategy has relied on communicating to rivals that any aggression would either fail or provoke a devastating counterattack—deterrence in a nutshell."[34] That said, the problems with excessive reliance on this model in the cyber context (not to mention post-Cold War international relations more generally) include the relatively low cost of attacking compared to the high cost of defending; problems of attribution (leading to delayed responses and the risk of being deceived by "false flag" operations); and the multiplicity of adversaries with varying degrees of connection to, and control by, foreign states.[35]

As many critics have noted, however, despite the pervasiveness of the war frame as a metaphor, malicious cyber acts do not fit neatly within it. As Thomas Rid wrote in *Cyber War Will Not Take Place*, the traditional Clauswitzian definition of war has not been met in the malicious cyber acts often offered as examples

31. James N. Miller & Neal A. Pollard, *Persistent Engagement, Agreed Competition and Deterrence in Cyberspace*, LAWFARE (Apr. 30, 2019), https://perma.cc/DE5Q-V6LH.

32. Jason Healey, *Taking Down Russian Trolls is My Kind of Cyberattack,* CIPHER BRIEF (Feb. 28, 2019, 9:12 AM), https://perma.cc/5EA6-RM93. To this end, Michèle Flournoy and Michael Sulmeyer have proposed creating "a new cyberdefense agency whose purpose would be not to share information or build criminal cases but to help agencies, companies, and communities prevent attacks." Michèle Flournoy & Michael Sulmeyer, *Battlefield Internet: A Plan for Securing Cyberspace*, FOREIGN AFF. (Sept./Oct. 2018), https://perma.cc/9XFX-N63X.

33. *See, e.g.*, Jacob Nagel & Jonathan Schanzer, *Assessing Israel's Iron Dome Missile Defense System*, FOUND. FOR DEF. DEMOCRACIES (Nov. 13, 2019), https://perma.cc/D55W-R3DS (discussing advantages and drawbacks of the system).

34. Andrew F. Krepinevich, Jr., *The Eroding Balance of Terror: The Decline of Deterrence*, FOREIGN AFF. (Jan./Feb. 2019), https://perma.cc/G8K9-HY3V; *see also* Jonathan Solomon, *Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?*, STRATEGIC STUD. Q., Spring 2011, 1-25 (assessing challenges for punitive cyberdeterrence and concluding that "cyberdeterrence by denial may actually be the stronger and more credible strategic path for the United States").

35. To be fair, these problems are not entirely unique to the cyber "domain." As Dorothy Denning observes with respect to land, sea, air, space, *and* cyber: "all are domains of human practice, characterized by a wide range of activity by both state and nonstate actors, some of which is hard to attribute, and by a variety of weapons ranging in availability, cost, and effects produced." Dorothy E. Denning, *Rethinking the Cyber Domain and Deterrence*, 77 JOINT FORCE Q. 8, 15 (April 2015). Additional complications arise from lack of clarity surrounding the international standards—legal or otherwise—governing the conduct of certain cyber activities that fall below the "use of force" threshold. *See, e.g.*, Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011); Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151 (2010).

of cyber attacks that amount to acts of war.[36] He lays out three criteria that, if present, would identify a cyber act as an act of war. First, war is an act of force to compel the enemy to do one's will. Second, war is instrumental and violence is the means for the attacker to achieve its ends. Finally, an act of war is always political in nature. Even to analyze MCAs through this frame, one must make certain assumptions about the nature of the actors and the environment in which they operate. Popular writers and even academic analysts view MCAs under the cyberwar frame, without examining whether these basic assumptions apply.

At their core, the laws of armed conflict developed to constrain the behavior of nation-states. As such, the framework assumes some basic characteristics of a given conflict, including (1) territoriality; (2) sovereignty; and, relatedly (3) the state's monopoly on the legitimate use of force. Yet, when applied to the experience of institutions confronting MCAs, these assumptions do not describe the environment in which malicious actions and responses occur.

**(1) Territoriality**. Deeply embedded in the international order is the idea of territoriality and control over physical space.[37] Historically, international armed conflicts often arose over contested territory.[38] The principle of territorial integrity enshrined in Article 2(4) of the United Nations Charter establishes the sanctity of territory as a cornerstone of peace. However, MCAs challenge the centrality of territory. The internet is everywhere and nowhere at the same time. The physical layer has locality, with wires and cables flowing across physical territory, and servers and terminals located within specific jurisdictions, but actions and their effects are not necessarily determined or limited by those locations.[39] Due to the migration to cloud computing and platform-based access, MCAs can be viewed as occurring wherever the actor is located (which can be spoofed to an alternate location), or wherever the victim experiences the consequences. As some have noted, data have no intrinsic territoriality.[40]

A cyberattack dreamed up in St. Petersburg and executed in Macedonia across servers located in Poland or Ireland, against an office in Washington, D.C. but

36. THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 1–4 (2013).

37. Dominic D.P. Johnson & Monica Duffy Toft, *Grounds for War: The Evolution of Territorial Conflict*, 38 INT'L SEC. 7 (2013).

38. *Id.*

39. Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317, 322-25 (2015).

40. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015). It is easy to become tied up in knots thinking about jurisdiction in cyberspace. That said, at a basic level, MCA involves (1) one or more human beings (2) giving instructions via computers to (3) produce a result, whether that result involves purely digital effects (e.g., stealing bitcoin) or changes the behavior of another human being (e.g., by eliciting a response to a fraudulent request). Results that involve changing human behavior are sometimes referred to as "cyber-enabled" or "internet-enabled" crime. *See, e.g.*, Neil Desai, *Tackling Cyber-enabled Crime Will Require Public-Private Leadership*, https://perma.cc/WX9B-END3 (visited Jan. 18, 2021). Regardless of the label, there are one or more perpetrators, and one or more direct or indirect victims. Both perpetrator(s) and victim(s) are subject to the laws of one or more nation-states based on ties of nationality and/or territory. In the absence of an international judicial system, attaching legal consequences to conduct that violates those laws falls to the domestic authorities of one or more of those states.

accessed remotely in Cancun poses serious challenges to a territorially-based conception of jurisdiction, let alone armed conflict. It is theoretically possible for nation-states to categorize and respond to MCA based on the location of the attack's origin and its effects. However, the originating territory is not always clear and often can't be identified quickly, thus undermining traditional deterrence models that depend upon swift and accurate responses.

**(2) Sovereignty**. Underlying the traditional model of international armed conflict is the principle of Westphalian sovereignty—the idea that states can control what happens domestically while adhering to principles of non-intervention across international borders. But the borderless, ubiquitous nature of the internet means that in this space notions of Westphalian sovereignty do not readily apply. While states may have the notional ability to regulate actions originating in their territory through application of local laws and regulations, most governments currently have little ability to prevent impacts within their territory of actions taken elsewhere through cyberspace.

Further, because the infrastructure of the internet was largely created and is currently maintained by private sector actors, the ability of states to control cross-border data flows is largely hindered by a lack of control over both the mechanisms and the content of the internet. In particular, where technology and internet companies provide multinational platforms, individual users may take actions that are prohibited within an impacted country but are legal where the user is located. For example, a comedy show taped in Manhattan, New York and uploaded by a company in Los Gatos, California can reach a global audience, some of whom may find that the content violates local speech laws.[41] Because states have much less of a monopoly on cyber infrastructure and activity than they do on weapons and their use, the ability of a state to maintain domestic control of cyber activity relies on cooperation from civilian commercial entities.

**(3) State monopoly on legitimate use of force.** The biggest challenge to viewing MCAs through a cyberwar lens is that the laws governing the resort to armed force traditionally assume that states have a monopoly on the legitimate use of force. Historically, part of the definition of being a state is the ability to control force emanating from within one's territory. Command and control, organization into armies, and use of uniforms all signal that a state, not an individual, has authorized the actions being taken.

This does not mean that all uses of military force are actually controlled by the state, but states traditionally had sufficient control to serve as effective international gatekeepers. Classical theories of deterrence, including in the nuclear arena, have developed on the theory that it is the sovereign ruler—whether an elected leader or a dictator—who is in control of either initiating or responding to the use of force. Military planners could generally rely on certain assumptions about the cause-and-effect relationship between their strategies and the desired

41. Jim Rutenberg, *Netflix Bow to Saudi Censors Comes at a Cost to Free Speech*, N.Y. TIMES (Jan. 6, 2019), https://perma.cc/8ATD-YRWH.

outcomes. But in the cyber domain, many of the MCAs that occur are conducted not by states but by private actors looking for gain, stealing information, or even just demonstrating proof of concept. From the perspective of the victimized entity, the effect may be clear, but the motive may not be. Indeed, there is a spectrum of state involvement in the cyber domain, from unsanctioned criminals, through "patriotic hackers," all the way up to national armies.[42] Each of these groups might be susceptible (or not) to different types of coercive responses, just as the states hosting such groups (either deliberately or inadvertently) might be amenable (or not) to direct responses by affected states. The situation is complicated even further by the current lack of a clear, shared understanding about the types of cyber activities that are, and are not, prohibited on a global scale, even though many countries have at least codified restrictions on criminal uses of the internet in their domestic laws.

Further, when it comes to online malicious acts, the state does not have the same degree of monopoly on the use of force that it does with either conventional or nuclear weapons. First, the development and use of so-called "cyber weapons" and the execution of code are not limited to government weapons designers. The code through which exploits are used are designed and built by private, commercial engineers outside of the defense contracting context. There is now a robust private sector market for the same kinds of offensive tools used by governments, which can now be used to target private companies and individuals. Criminals on the darkweb trade in tools designed to exfiltrate data, interrupt services, and build ransomware attacks. Even when states design, build, and stockpile cyberweapons, they cannot guarantee exclusive control of their tools.[43] States are unwilling to engage in the same kinds of transparency and verification regimes of their cyber-tools to demonstrate their exclusive control. In the absence of a state monopoly on the use of force, the idea of state-to-state deterrence as an effective solution to curbing cyber conflict is unlikely to yield a cessation of hostile activity.

In sum, discussions of "cyberwar" tend to over-emphasize military responses as well as the development of rules of conduct analogous to the rules of armed conflict. This can crowd out thinking about MCA through other frames and developing other institutional responses.

## III. CYBERWAR VS. CYBERCRIME

The threat of *cyberwar*, and the pervasiveness of *cybercrime*, require vigilance and action by government and the private sector (which controls vast swaths of critical infrastructure). An armed conflict model of deterrence can provide a framework for addressing certain types of cyber-threats from hostile nation-states that we might

42. *See* HEALEY, *supra* note 19.

43. *See* Bruce Schneier, *Who Are the Shadow Brokers? What Is-And Isn't—Known About the Mysterious Hackers Leaking National Security Agency Secrets*, ATLANTIC (May 23, 2017), https://perma.cc/5DT7-RDN4.

think of as falling into the "war" category. It does little, however, to address the dangers posed by cybercrime. Currently, private sector incentives to invest in cybersecurity include the reputational costs associated with breaches; business losses associated with impaired functionality; and potential regulatory and tort liability.[44] The law enforcement infrastructure required to support these efforts has not kept pace with the scale of the threat or the degree of danger it poses.

The conceptual and doctrinal framework used to differentiate between "armed attacks" that give rise to the right of self-defense under U.N. Charter Article 51 and all other types of conduct is notoriously difficult to apply in the cyber context.[45] Moreover, even if relevant actors agree on whether the result of a particular cyber operation is the functional equivalent of a kinetic "attack" for Article 51 purposes, delays and ambiguity in attribution further complicate the picture. Although engaging in debates about the appropriate "control" test for attribution remain beyond the scope of this article, attributing MCA—and substantiating that attribution without revealing sources and methods—can impede efforts to expose and punish individual wrongdoers and the states that may direct or support them.[46]

While individuals may bear criminal responsibility under both international and domestic law, state responsibility has generally been understood as non-criminal in nature.[47] A state might owe a duty of cessation, restitution, reparation, or satisfaction, but states are not generally subject to penal sanctions. Individuals, on the other hand, can and do bear individual criminal responsibility for violations of both domestic and international criminal law—often, even when they were acting at the direction, or on behalf, of a foreign state. States are beginning to navigate the difficult terrain of imposing criminal penalties on individuals for carrying out state policy—something that the doctrine of foreign official

---

44. *See*, *e.g.*, Nathaniel Sobol, *The SEC and Cybersecurity Regulation*, LAWFARE (Nov. 19, 2018), https://perma.cc/H9YB-87GP; Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J. L. REFORM 913 (2017); Robert L. Rabin, *Perspectives on Privacy, Data Security, and Tort Law*, 66 DEPAUL L. REV. 313 (2017); *but cf.* Stewart Baker, *Why Tort Liability for Data Breaches Won't Improve Cybersecurity*, VOLOKH CONSPIRACY (Jan. 11, 2015), https://perma.cc/M2WD-B2PP (noting that "the actual damages from data breaches are pretty modest in dollar terms, and the pattern of losses makes it very hard to sustain a single class, something that forces up the cost of litigation for the plaintiffs").

45. *See, e.g.*, Kubo Mačák, *Scenario 13: Cyber Operations as a Trigger of the Law of Armed Conflict*, CYBER LAW TOOLKIT, https://perma.cc/UA4F-Q57K (last edited Jan. 14, 2020). On the question of identifying the threshold for an international or a non-international armed conflict, *see* Laurie R. Blank & Benjamin R. Farley, *Identifying the Start of Conflict: Conflict Recognition, Operational Realities and Accountability in the Post-9/11 World*, 36 MICH. J. INT'L L. 467, 478-87 (2015). This question also has implications for the cyber insurance market, as illustrated by the *Mondelez* case involving whether a policy's exemption for "hostile or warlike" actions covers damage from the NotPetya virus. *See* Brian Corcoran, *What* Mondelez v. Zurich *May Reveal About Cyber Insurance in the Age of Digital Conflict*, LAWFARE (Mar. 8, 2019, 8:00 AM), https://perma.cc/7XNS-BLH6.

46. On attribution generally, *see, e.g.*, Kristen E. Boon, *Are Control Tests Fit for the Future? The Problem in Attribution Doctrines*, 15 MELBOURNE J. INT'L L. 1 (2014).

47. *See, e.g.*, Chimène I. Keitner, *Categorizing Acts by State Officials: Attribution and Responsibility in the Law of Foreign Official Immunity*, 26 DUKE J. COMP. & INT'L L. 451, 461 (2016) (noting that state responsibility in international law has traditionally been understood as the functional equivalent of "liability" in municipal law).

immunity has traditionally sought to avoid. Just as targeted sanctions attempt to influence state behavior by pressuring individual foreign officials, so too does the threat of prosecution aim to dis-incentivize individuals from engaging in MCA, even on behalf of foreign states. The traditional distinction between "official" or "public" acts, on the one hand, and "private" acts (such as those taken for personal benefit or financial gain), on the other, has already come under pressure with the increasing recognition of the need to prosecute and punish international crimes. The widespread phenomenon of state-sponsored cybercrime promises to further challenge, and perhaps erode, this distinction, at least in certain contexts.

## IV. TOWARDS A GLOBAL LAW ENFORCEMENT MODEL

Given the difficulty in achieving international consensus and cooperation, the Budapest Convention on Cybercrime (CETS No. 185) remains the only binding international instrument on cybercrime. It serves as a guideline for countries developing national legislation against cybercrime, and it seeks to provide a framework for international cooperation between states parties to the treaty. The Cybercrime Convention Committee meets twice per year in an effort to facilitate the effective use and implementation of the Convention, and to consider future amendments.[48] However, the Convention's reach is far from global, and does not include China or Russia. In addition, problems persist in securing agreement on provisions that would facilitate investigations, prosecutions, and extraditions without impinging unduly on privacy and human rights. Alexander Seger, Executive Secretary of the Cybercrime Convention Committee, has written:

> With cyberspace considered the "fifth domain of warfare" considerable resources are allocated by States to defensive and offensive military capabilities and information operations, with the obvious risk of a further militarisation of cyberspace. Criminal justice obviously offers a higher level of protection of the rights of individuals than national security or defence solutions. However, the very need to protect the rights of individuals and to meet data protection and other rule of law requirements may very well lead to a dilemma: if criminal justice authorities are no longer able to investigate cybercrime and secure electronic evidence in an effective manner, competencies and resources may further shift to national security and intelligence bodies without the same level of safeguards.[49]

Despite these challenges, domestic law prohibitions on unauthorized cyber activity are relatively well-established. Building the capacity to enforce these

48. *See T-CY Plenaries*, COUNCIL OF EUR., https://perma.cc/L9CE-8XQ5.

49. Alexander Seger, *Enhanced Cooperation on Cybercrime: A Case for a Protocol to the Budapest Convention,* ITALIAN INST. FOR INT'L POL. STUD. (July 16, 2018), https://perma.cc/94V3-Y6WB. For concerns about the recent passage of a Russia-sponsored U.N. resolution on cybercrime that threatens an "open, free, and secure model of the internet," see Joyce Hakmeh & Allison Peters, *A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet*, COUNCIL ON FOREIGN REL. (Jan. 13, 2020), https://perma.cc/MD9T-WF7H.

prohibitions requires adequate resources and training at the domestic level, as well as multinational cooperation in evidence-gathering and, potentially, apprehension of suspects when MCA crosses borders, as it regularly does.

A recent Council on Foreign Relations report underscores the importance of capacity-building under a law enforcement framework, noting:

> A common misperception is that the principal cybersecurity threats demanding urgent international collaboration are massive, state sponsored attacks that target critical infrastructure such as power plants or electrical grids, causing massive devastation and human casualties. In fact, cyber threats are more diverse and complex, often targeting private enterprises and endangering the technical integrity of the digital world. The near-total digitization of business models makes the global economy more vulnerable to cyberattacks, not only from states but also from criminal organizations and other nonstate actors.[50]

The engagement of intergovernmental organizations such as Interpol,[51] the United Nations Office on Drugs and Crime,[52] the International Telecommunications Union,[53] and the Council of Europe[54] in coordination and capacity-building efforts remains critical in expanding domestic capabilities, with due regard for human rights concerns.[55] Nongovernmental organizations, such as the Global Cyber Alliance, also have an important role to play.[56]

The technical and logistical difficulties of deterring garden-variety cybercrime should not be underestimated, but this is a reason to devote more—not fewer—resources to the effort. Joshua Tromp has described the challenge of deterring cyberattacks in the following colorful terms:

---

50. Council on Foreign Relations, *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms* (Feb. 23, 2018), https://perma.cc/R6W3-V4HR.

51. INTERPOL, CYBERCRIME, https://perma.cc/9PKT-LHWT.

52. CYBERCRIME, UNITED NATIONS OFF. ON DRUGS & CRIME, https://perma.cc/39PB-YL8N; *see also* UNITED NATIONS OFF. ON DRUGS AND CRIME, COMPREHENSIVE STUDY ON CYBERCRIME (Feb. 2013), https://perma.cc/PPL9-D3Z8.

53. *ITU-D Cybersecurity*, INT'L TELECOMMS. UNION, https://perma.cc/F8KY-SFZV.

54. COUNCIL OF EUROPE, ACTION AGAINST CYBERCRIME, https://perma.cc/R4YJ-JCUW.

55. *See, e.g.*, Myrian Dunn Cavelty & Camino Kavanagh, *Cybersecurity and Human Rights*, *in* BEN WAGNER, MATTHIAS C. KETTEMANN & KILLAN VIETH (eds.), RESEARCH HANDBOOK ON HUMAN RIGHTS AND DIGITAL TECHNOLOGY, ch. 5 (2019) (exploring the relationship between cybersecurity and human rights); Ronald J. Deibert, *Towards a Human-Centric Approach to Cybersecurity*, 32 ETHICS & INT'L AFF. 411 (2018) (advocating for an approach to cybersecurity that prioritizes the individual rather than the state, including by creating multiple forms of independent oversight and review); Andrew N. Liaropoulos, *Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance*, 6 INT'L J. OF CYBER WARFARE & TERRORISM 33 (2016) (arguing that the dominance of war metaphors in cyber security discourse has failed to address the needs of people). For interventions from civil society groups, *see*, *e.g.*, *How Law Enforcement Can Access Data Across Borders—Without Crushing Human Rights*, IFEX (July 4, 2018), https://perma.cc/2HYW-2X8F; *Mapping Cybercrime Laws and Violations of Digital Rights in Gulf and Neighboring Countries*, GULF CENTRE FOR HUMAN RIGHTS (June 26, 2018), https://perma.cc/L3HZ-DWWZ; Anja Kovacs & Dixie Hawtin, *Cyber Security, Cyber Surveillance and Online Human Rights* (May 2013), https://perma.cc/UN9W-SJ7W.

56. GLOBAL CYBER ALLIANCE, MISSION & PURPOSE, https://perma.cc/7CTN-KZK9.

> Comparing cyber-attacks to the analogy of a child stealing cookies from a cookie jar, the current environment is one where a child knows he should go ahead and steal the cookie. The child's parents are unable to determine who took the cookie or in many cases to even notice a cookie is missing. And the parents are severely limited in enacting any significant punishment for taking the cookie. For the child, the benefits are great and the costs are low.[57]

Although Tromp argues for clearer deterrent options under an armed conflict model, the "deterrence by punishment" approach under a law enforcement model also has much to commend it. In both cases, a core problem today is the lack of certainty that punishment will ensue—to the contrary, the likelihood of detection of malfeasance and follow-through by authorities is vanishingly small.[58]

Duncan Hollis suggested in 2011 that features endemic to MCA make it futile to rely on strategies of deterrence by proscription and punishment. In his view, "[i]f cyberattackers assume that they cannot be identified (let alone sanctioned), rules prohibiting cyberattacks and exploits will have little deterrent effect."[59] Eric Jensen, by contrast, has characterized deterrence via the imposition of criminal or civil penalties as a form of "legal strike back."[60] As Jensen emphasizes, however, "legal strike back can only be an effective means of deterrence when states work together with the common goal of suppressing malicious cyber activity."[61] For this reason, a law enforcement model of deterrence must also involve an emphasis on diplomatic efforts to prioritize and to incentivize international cooperation.

In addition to problems of insufficient capacity, coordination, and consensus, a complication also arises from the fact that some highly-publicized MCA appears to be carried out by individuals at the direction, and/or with the tacit support, of the very states that are charged with suppressing and punishing MCA. Any steps that the United States takes to punish individuals involved in these efforts, or to hold states responsible for failure to suppress MCA emanating from their territory, will raise questions of the degree to which the United States is willing to subject itself, and its personnel, to similar enforcement efforts undertaken by other states. This is one of the many reasons that cooperative approaches, where possible, are likely to yield more sustainable results than unilateral measures. Moreover, the potentially sensitive diplomatic issues raised by these high-profile cases should not detract from efforts to combat the large swath of MCA that is not sponsored or directed by states, as illustrated by the figure below.

---

57. Joshua Tromp, *Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-Attacks*, SMALL WARS J. (2016), https://perma.cc/5DXC-XRMP.

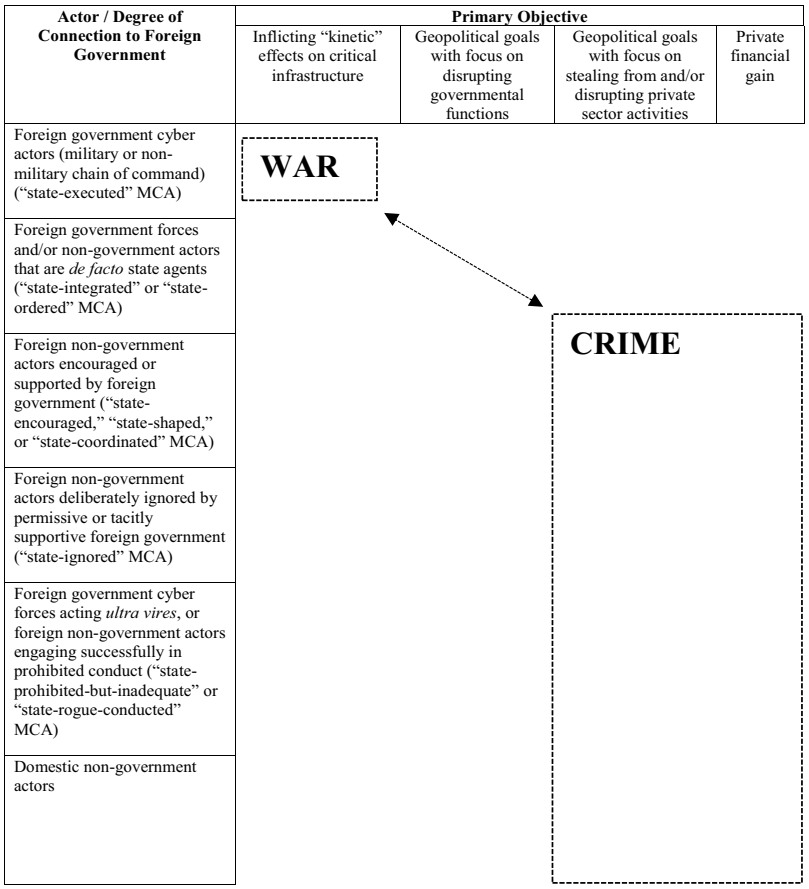
58. Although empirical research on deterrence faces numerous methodological challenges, criminologists have concluded in a number of studies that declining crime rates are associated with an increased likelihood (certainty) of apprehension and punishment. *See Five Things About Deterrence*, NAT'L INST. OF JUST. (June 5, 2016), https://perma.cc/55TW-33WC; *see also* Kelli D. Tomlinson, *An Examination of Deterrence Theory: Where Do We Stand?*, 80 FED. PROBATION 33 (Dec. 2016), https://perma.cc/Q38B-W7DV.

59. Duncan Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L. J. 373, 378 (2011).

60. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 800 (2012).

61. *Id*. at 806.

**Fig. 2**
**Disaggregating Threats & Responses: A War/Crime Continuum**




By disaggregating and differentiating among different types of MCA, including by their provenance, goals, and (where ascertainable) motivations, we can move towards a more comprehensive and coordinated response to this ever-growing problem.