Four Big "Ds" and a Little "r": A New Model for Cyber Defense

Matthew Cohen, Chuck Freilich, Gabi Siboni

As with all emerging threats, the cyber realm represents new dangers, which will be difficult to address. This article argues that cyberthreats are not fundamentally different from other asymmetric threats, and it provides a conceptual model for developing a response by drawing on classic principles of military strategy, the "four Ds"—Detection, Deterrence, Defense, and Defeat—as well as resilience (the little "r"). We offer a model for how countries can create policies addressing each of these principles that will enhance the security of national cyber systems. The proposed framework will allow for the development of detailed strategies and plans to address the specific demands posed by cyberthreats, whether state-based, or by non-state actors, or individuals.

Keywords: cyber, detection, deterrence, defense, defeat, resilience

Introduction

Cyberspace is a dangerous place for nations. In 2016 a group called the "Shadow Brokers" announced it had successfully stolen classified malware codes used by the United States' highly secretive National Security Agency. Some of this code, which is used to conduct espionage, is currently available to download online, and the Shadow Brokers have offered to sell the rest

Matthew Cohen is a PhD candidate and lecturer in Political Science at Northeastern University. Dr. Chuck Freilich, a senior fellow at Harvard's Belfer Center, is a former deputy national security adviser in Israel. Gabi Siboni is a senior research fellow and head of the Program on Military and Strategic Affairs and Program on Cyber Security at INSS.

of the information to anyone willing to pay their hefty asking price.[1] In 2015, the United States announced that hackers had infiltrated sensitive computer systems at the White House, calling it one of the most sophisticated cyberattacks ever launched on US government systems; Russia is the likely culprit.[2] That year, North Korea launched a cyberattack against South Korea's nuclear operator, raising concerns regarding the safety of its nuclear power plants.[3] In 2014, hackers attacked Sony servers, posted private emails, and issued violent threats against the company and against any theater screening a satirical movie about North Korea. The United States blamed North Korea for the attack, stating that it would respond in a "proportional manner," and shortly thereafter North Korea's internet service was disrupted for days.[4] These are just a small sample of recent cyberattacks.

This article argues that the cyberthreat does, indeed, have some particularly difficult characteristics, but that an effective response can and will be found. To do so will require that a conceptual model be formulated to frame and guide discussion of the severity of different cyberthreats, the technologies to be developed, and the necessary government policies. This article proposes such a conceptual model by drawing on the classic principles of military strategy, the "four Ds"—Deterrence, Detection, Defense, and Defeat—as well as the less well-known concept of resilience (the little "r"). It will further explore how governments, militaries, and private entities can work together within this framework to address threats in cyberspace.

The concept of the four Ds is widely known and applied by governments around the world, but is defined differently by various authors and nations. For example, the United States applied a four Ds model, "defeat, deny, diminish, and defend," to the threat of terrorism in its 2003 "National

1 Paul Szoldra, "New Snowden Documents Prove the Hacked NSA Files are Real," *Business Insider*, August 19, 2016, http://www.businessinsider.com/snowden-confirm-hacked-nsa-files-2016-8.

2 Evan Perez and Shimon Prokupecz, "How the U.S. Thinks Russians Hacked the White House," *CNN*, April 8, 2015, http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html.

3 K.J. Kwon, "Smoking Gun: South Korea Uncovers Northern Rival's Hacking Codes," *CNN*, April 22, 2015, http://www.cnn.com/2015/04/22/asia/koreas-cyber-hacking/index.html.

4 Haroon Siddique, "North Korea Responds with Fury to US Sanctions Over Sony Pictures Hack," *Guardian,* January 5, 2015, http://www.theguardian.com/world/2015/jan/04/north-korea-fury-us-sanctions-sony.

Strategy for Combating Terrorism."[5] Another example is Israel, which based its national security strategy for decades on a three Ds model of detection, deterrence, and defeat,[6] and later introduced a fourth "D,"—defense—for cyberthreats, as well.[7]

To date, no study has applied a comprehensive strategy of four Ds to the cyberthreat, although studies have touched upon each of the Ds separately. Each study offers valuable insights into the cyber realm, but the four Ds and the concept of resilience have interconnecting components that may be missed by surveying them separately. Thus, a holistic analytical framework that examines them together can offer a more complete understanding of the cyberthreat, both for academic and policymaking purposes.

Defining the Cyber Realm

Many terms regarding cyberspace lack clear and widely accepted definitions. For our purposes, a cyberattack is an offensive use of cyberspace that both uses and targets computers, networks, or other technologies for malevolent, destructive, or disruptive political or criminal purposes.[8] Politically motivated cyberattacks—like other forms of warfare—aim to provide a strategic, diplomatic, economic, or military advantage over an adversary, or to force it to take an action it does not want to take.[9] Cyberattacks can be launched

5 US State Department, "National Strategy for Combating Terrorism," February 2003, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

6 Matthew S. Cohen, Chuck Freilich and Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response," *International Studies Perspectives* 17 (2016): 307–321; Chuck D. Freilich, "Why Can't Israel Win Wars Anymore?" *Survival* 57, no. 2 (2015): 79–92.

7 Chief of the General Staff, "The IDF Strategy," *Israel Defense Force*, July 2016, https://www.idfblog.com/s/Desktop/IDF%20Strategy.pdf.

8 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Rand Corporation: Project Air Force, 2009); Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2012); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

9 Jeffrey Carr ed., *Inside Cyber Warfare* (Cambridge: O'Reilly, 2012); Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2011): 817–886; Valeriano and Maness, *Cyber War versus Cyber Realities*.

by nations, non-state organizations, or individuals. Cyber defense includes efforts to ensure the ability to maintain control of internet service providers (ISP) and incoming and outgoing traffic, and to halt ongoing attacks.[10] Cyber espionage refers to use of the cyber realm by the state or by national security agencies (NSA) (often via malware or hacking, such as spear-phishing) to steal or gather information, or make known the attackers' ability to penetrate networks.[11]

Four Big "Ds" and a Little "r"

In this section, we argue that, with some adaptations, cyberthreats can be effectively addressed using fundamental principles of military strategy—the above-mentioned four Ds, and the newer concept of resilience.

Deterrence. In order to deter an adversary, the adversary must have an identifiable "return address" against which to retaliate, and attribution must be possible, which is especially difficult in the cyber realm. Deterrence is further complicated in the cybersphere by the fact that it is not always possible to tell when damage has been done; indeed, the target may not even know it has been attacked.[12]

Different levels of certainty of attribution determine the type of response the country should deploy. A comparatively low level of certainty is all that is required for behind-the-scenes diplomacy. In such cases, a country can accuse another of attempting to modify its behavior without definitive proof. A medium level of certainty would be necessary before making public accusations. The highest level of certainty is needed for undertaking legal or kinetic action.

In cases of cyberattacks in which attribution is possible, the type of actor (state, terrorist group, NSA, or individual) plays an important role in determining the nature of the deterrence policy. Deterrence of cyberattacks by state actors is not substantively different from deterrence in other conflicts. The state under attack can retaliate with the entire spectrum of capabilities at its disposal— cyber, diplomatic, kinetic, or economic.

---

10 Chris C. Demchak, *Wars of Disruption and Resilience* (Athens: University of Georgia Press, 2011); Valeriano and Maness, *Cyber War versus Cyber Realities*.

11 P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014); Valeriano and Maness, *Cyber War versus Cyber Realities*.

12 Libicki, *Cyberdeterrence and Cyberwar*.

Deterring cyberattacks by terrorist groups is similar to preventing physical attacks, again running the gamut of potential cyber and non-cyber forms of retaliation. Most terrorist organizations are not nihilistic and have values they wish to protect, although the importance they attach to these values and their tolerance for punishment may be different from that of states. The ability to retaliate would only be limited by the same considerations that apply to the decision to employ physical retaliation, including distance and vulnerability. Just as in the physical world in which deterring terrorists is highly challenging, it is difficult to deter terror groups from launching attacks in cyberspace.

The sheer number of potential non-state organizations and individual attackers (hackers and activists) dispersed around the globe presents a challenge to the monitoring and attribution capabilities needed for purposes of deterrence. The sophisticated cyber capabilities of the state can, however, make it more difficult for an organization or individual to hide their identity. The good news regarding non-state organizations and individuals is that they are less likely to have the resources required to launch crippling cyberattacks against advanced states, and publicity is often one of their primary motivations, thereby facilitating attribution. Additionally, developing better forensic tools—an effort already underway—will help determine who launched the attack.

Detection. Detection or early warning of impending attacks is as critical in the cyber realm as in the physical. Prevention is only possible if there is sufficient early warning, and it is also usually easier to defend against such an attack. Few states, let alone NSAs, have the capabilities required to successfully conduct a major cyberattack against a sophisticated state-defender. The true challenge of detecting cyberattacks lies not in the vast number of potential attackers around the globe, but rather in the limited number of highly sophisticated ones; in this case, the problem of detection becomes more manageable.

Complicating the picture is the increasingly interconnected nature of governmental, military, and private-sector networks. Private-sector networks can now be used as a gateway to attack some governmental and military networks, meaning that the private sector should now be considered a vulnerability. Thus, states face the need to provide early warning not just for governmental systems and critical infrastructure, but also for major

organizations and companies. Nations have already begun employing increased intelligence-gathering efforts and have expanded information sharing with the private sector. Nevertheless, information sharing between governments and private companies remains a significant challenge. Encouraging such efforts will likely require legal, organizational, and political changes by both governments and companies.[13] Technology is a critical component of a nation's cyber detection systems. Such efforts will also be greatly strengthened by using traditional off-line intelligence gathering of potential attackers to supplement what is gathered online.[14]

Several factors work to the defender's advantage. Attackers often conduct "cyber-reconnaissance missions" to assess the weak points in the defender's systems.[15] The larger a planned or ongoing cyberattack is, the easier it is to intercept communications between the attackers and carry out defense. For many nations, the problem of detection is simplified by the small number of communications cables carrying internet traffic.

Defense. Defense addresses the prevention and mitigation of attacks on military, governmental, and critical infrastructure networks, as well as on private networks, businesses, and individuals. The source of the attack determines the best means of defending against it, as the various actors are capable of different types of attacks and levels of severity. As noted, it is generally more difficult to defend against attacks by states, whereas the technological capabilities of non-state organizations and individuals are typically less advanced and can be handled through simple technological solutions.

Technology plays a central role in defensive efforts, and states have already begun building programs to assist with the defense of networks and cyber systems. Developing a range of technologies capable of addressing all types of threats is, of course, ideal, but resource constraints will require states to prioritize which threats are the most pressing so that the states can focus their resources on them. This is another area in which governments and the private sector can work together. Doing so will boost their ability to

13 Aviram Zrahia, "A Multidisciplinary Analysis of Cyber Information Sharing," *Military and Strategic Affairs* 6, no. 3 (2014): 59–77.

14 Gabi Siboni and Ofer Assaf, *Guidelines for a National Cyber Strategy* (Tel Aviv: Institute for National Security Studies, 2016).

15 Ned Moran, "A Cyber Early Warning Model," in *Inside Cyber Warfare*, ed. Jeffrey Carr (Cambridge: O'Reilly, 2012).

identify the greatest threats and create new tools for defense. Governments can even benefit if private cybersecurity companies choose not to work with them by observing the threats the companies address and using that as a guide for the government's threat assessment efforts. Governments can additionally work with private entities to ensure that security systems on networks that connect to government systems are up-to-date.[16]

At the same time, cyberdefense cannot be conducted only online, but rather requires a multi-layered effort involving gathering intelligence, interrupting attacks, securing networks, undertaking legal measures, formulating new norms of behavior, and engaging in effective cooperation with foreign governments. Currently, no clear international norms or laws exist regarding behavior in cyberspace.[17] Treaties, laws, and norms could prove to be useful in limiting malicious actions by states in cyberspace. To be effective, states must agree on the types of activity to be addressed, the responsibilities of the state under the agreement, and the punishments for violations. In addition, states must establish international bodies to oversee compliance.[18]

International cooperation is also of great importance and states can benefit from deepening and expanding the number of nations they cooperate with on cybersecurity. Intelligence sharing, bilateral and multilateral agreements, and improved cooperation with law enforcement agencies in other countries can

16 William J. Lynn, "Defending a New Domain," *Foreign Affairs*, October 2010, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Milton L. Mueller, Andreas Schmidt, and Brenden Kuerbis, "Internet Security and Networked Governance in International Relations," *International Studies Review* 15, no. 1 (2013): 86–104; Ido Naor, "ATMZombie: Banking Trojan in Israeli Waters," *SecureList*, February 29, 2016, https://securelist.com/blog/research/73866/atmzombie-banking-trojan-in-israeli-waters/; Teri Radichel, "Case Study: Critical Controls that Could Have Prevented Target Breach," *SANS Institute*, 2014, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

17 Abraham D. Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," *Proceedings of a Workshop on Deterring Cyber-Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington DC: National Academies Press, 2010), http://www.nap.edu/catalog/12997.html; Valeriano and Maness, *Cyber War versus Cyber Realities*.

18 Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

be of great value in planning defensive strategies.[19] Enhancing cooperation between states will be necessary to ensure that new laws and norms are enforced.[20]

Defeat. The concept of defeat in the cyber realm should not be viewed as completely preventing all cyberattacks. In both the physical and cyber realms, decisive defeats have been quite rare. Defeat of an adversary in the cyber realm should thus be understood as reducing the number and severity of attacks to a level that allows a society to maintain its way of life and to bounce back quickly from attacks (see below for more on resilience). To achieve defeat in the cyber realm, a nation must be able to show its opponents that it can prevent major cyberattacks; cyberattacks that a state cannot prevent will be futile, either because they will not cause significant damage or the state is capable of rapidly bouncing back; and that cyberattacks will be met with some form of retaliation. Overall, achieving defeat requires that states be capable of successfully implementing each of the four Ds and the little r.

States must also give cyberattacks the same importance they attach to physical attacks and—when appropriate—use similar methods and strategies, such as responding not just with cybertools, but also with kinetic capabilities.[21] Launching kinetic attacks is straightforward against attacking states, but is far more complicated against NSAs, and would require either gaining the permission of the host-state or risking a military escalation. Additionally, there is likely to be significant public backlash against the use of kinetic strikes in response to cyberattacks by an NSA.

Due to the highly diffuse nature of the threat, nations cannot expect to prevent every cyberattack from every individual and non-state organization around the world. A nation can defeat an opponent in cyberspace by minimizing the likelihood of a major attack capable of widespread disruption or damage. If an adversary cannot successfully execute a major attack, it has, in effect, been defeated. For the numerous NSAs and individual attacks, defense is

19 Observer Research Foundation, "International Public Private Partnership in Cyber Governance (Panel)," in *CYFY Conference Report, 201*3, India Conference on Cyber Security and Cyber Governance, http://www.bic-trust.eu/files/2014/04/CYFY-2013-Report-WEB-version-15Apr14.pdf.

20 Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

21 Robert Hackett, "Let's Get Physical? United States Weighs Options When It Comes to Cyber Attacks," *Fortune*, May 12, 2015, http://fortune.com/2015/05/12/rogers-cyber-attacks-us-response/.

a more appropriate response and a better use of resources, particularly as they are unlikely to have the capabilities necessary to cause severe damage.[22] Enhanced international cooperation can improve the ability of states to defeat such actors by imposing legal and criminal penalties for cross-border attacks.[23] States can more realistically aspire to achieving cyber defeat of states, terrorist organizations, and major non-state organizations.

Resilience. If an attack succeeds, the question is then how to manage the damaged system and to recover as rapidly as possible, i.e., to build "resilient" systems. Different systems will require differing levels of resilience. Some networks only need to quickly return to their most minimal level of functioning, while others must return to their original level of functioning as soon as possible.

The process of building resilient systems in cyberspace starts by drafting various high probability but low-cost scenarios, as well as low probability but high cost ones. Once developed, it is then possible to build plans and tools to address them. This must take place before failures occur and should include technological measures, human resource development, training exercises and drills, and implementation measures.[24] Resilience in the context of the cyber realm must also include plans regarding how to recover from the physical effects of cyberattacks.

The inherent limit on resources means that it is critical to prioritize the systems that require resilience. For example, military systems and the power grid likely are far more important to a nation than other networks. Metrics can be developed to help determine which systems are most critical and thus where to invest technological resources.[25] The impact of a failed network or infrastructure on the public morale and the citizens' faith in their government to provide basic public goods is one important measure to consider.

Building resilience also requires working closely with the private sector. Private companies are often responsible for maintaining facilities, dealing with threats, and ensuring they continue to operate. Governments must work

22 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy* 4, no. 63 (2010): 63–86.

23 Valeriano and Maness, *Cyber War versus Cyber Realities*.

24 P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford University Press, 2014); Valeriano and Maness, *Cyber War versus Cyber Realities*.

25 Ibid.

with, as well as regulate, the private sector to ensure that the facilities have proper plans in place for addressing failures.[26]

Reality is likely to present unexpected cyberdefense failures, with results that may be extreme; a resilient system could be the difference between relatively rapid recovery and severe consequences. Intelligence gathering of enemy plans or more generally their capabilities can be vital in planning the recovery.[27] Resilient systems make attacks far less consequential, thereby reducing the payoff for the attacker.[28] This, in turn, decreases the likelihood that an attack will occur in the first place.

Resilience can, however, only go so far, and eventually an attack will take down both a system and the response designed to deal with its failure. Nations must be prepared for this likelihood and should develop additional plans for living without the system for a more extended period. This will likely require redundancy and will require policymakers to develop plans that are not dependent upon technology.

Policy Implications

In this section, we discuss specific policy recommendations drawn from the four big Ds and little r model. To achieve deterrence, nations must make it clear to their adversaries what their retaliatory capabilities may be and the penalties they are likely to pay. Deterrence postures and intentions can be made through public statements and/or confidential channels.[29] This is complicated by problems of determining attribution as it is not always clear who should be the target of these postures and intentions. This can be overcome, however, as attribution abilities improve. Improved attribution abilities will convince the target of the deterrence postures that they will

26 Dana Pasquali, "3 Steps Towards Building Cyber Resilience into Critical Infrastructure," *Dark Reading*, August 2, 2016, http://www.darkreading.com/vulnerabilities---threats/3-steps-towards-building-cyber-resilience-into-critical-infrastructure/a/d-id/1326464; Jan Trobisch, *Challenges in Protection of US Critical Infrastructure in the Cyber Realm* (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 2014), https://www.hsdl.org/?abstract&did=791151.

27 Demchak, *Wars of Disruption and Resilience*.

28 US Department of Defense, "The DoD Cyber Strategy," 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

29 Ibid.

suffer the penalties, in addition to helping states to target their policies more effectively to the relevant adversaries.

The nature of the government in the country from which a cyberattack originates and, specifically, its willingness to cooperate are both crucial factors. Here, retaliation is not possible, unless the attacked state is willing to breach the sovereignty of the country that hosted the cyberattackers. Instead, a nation may be able to achieve deterrence by working with the host government's intelligence and law enforcement agencies. In some cases, the likelihood of severe legal action might be a sufficient retaliatory deterrent. Today, this expectation is quite limited, thereby emboldening organizations and individuals to carry out cyberattacks. When attacks originate in countries that do not have cooperative or effective governments, the ability of a nation to deter through legal means is, of course, far more limited. The deterrent question then becomes similar to retaliation against a physical attack and revolves around whether the attacker has cyber capabilities or other values that are worth counterattacking and the feasibility of doing so.

The real problem in deterring NSAs in the cyber realm, as in the physical world, may be that the damage they cause—painful as it may be—is usually limited, while their tolerance for pain often exceeds what the responding state is willing to mete out as punishment. This is especially true of Western democracies. It is not that they are incapable of defeating NSA threats; rather, the effort required to defeat them—including the level of damage and cost in lives—typically has been perceived as incommensurate with the threat to the state's interests. The same holds true for cyberattacks. Should an NSA conduct a drastic cyberattack, or should there be convincing information about an impending one, the country under attack undoubtedly will be more willing to adopt severe deterrent measures. To achieve deterrence, states must be able to assign attribution for an attack. To this end, states must deploy and continuously improve technological and intelligence tools, including information gathering about the technological abilities and goals of potential adversaries.[30] This is an area in which private entities and governments

30 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

should consider ways to work together, as private cybersecurity companies can identify malware and offer insights into its possible origins.[31]

A further complication is that cyberattacks may be routed through ISPs in third-party nations. It is possible for a government to work with or pressure the ISPs or their host governments to halt cyberattacks as they occur.[32] If adequate cooperation is not achieved, it may be possible to retaliate by publicly shaming the state, group, or individual that conducted the attack. This has the additional benefit of alerting security services around the world to the attacker, thus decreasing their ability to launch further attacks.

Efforts to improve the detection of cyberattacks should be based both on specially tailored means of gathering cyber intelligence and investing a greater portion of already existing human and electronic intelligence resources in the cyber realm. As much as cyber technology poses new problems of detection, it also provides new options for doing so.[33] The Australian national cyber strategy stresses this point and calls for improved detection through continuous online, real-time monitoring.[34] Although a vast number of cyberattacks can be launched simultaneously from different sources, cyber technology can detect and counter a similarly large number. One option, appropriate primarily for non-state and individual attackers, is to pose as fellow activists and members of the cyber networks in order to gain intelligence, skills, and tools.[35]

A difficulty in detecting attacks by both states and NSAs is that they can originate in friendly nations, which constrains the ability to spy on them without straining relations. Technology, however, can assist with this, since detection can be done from afar without violating a state's sovereignty.

---

31 Grant McCool, "Computer Spying Malware Uncovered with 'Stealth' Features: Symantec," *Reuters*, November 23, 2014, http://www.reuters.com/article/us-symantec-malware-regin-idUSKCN0J70SH20141123.

32 Clarke and Knake, *Cyber War*.

33 Department of Homeland Security, "The National Strategy to Secure Cyberspace," February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

34 Commonwealth of Australia, "Australian Government Cyber Security Strategy," 2009, http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

35 Microsoft, "Impersonation," http://technet.microsoft.com/en-us/library/cc961980.aspx.

Conversely, the need for heightened international cooperation and information sharing is clear.

In terms of defense, states wishing to bolster their capabilities can focus on improved use of technology. Defending the cyber realm demands that existing technologies be improved and new ones be created. The defense mechanism must also be appropriate for the situation. In the initial stages of an attack, before any real damage has been done or systems penetrated, efforts to disrupt or redirect the attack may be adequate. If the system has been penetrated, or damage done, the defense mechanism should seek to contain the attack, as well as prevent the attacker from knowing that the intrusion has been discovered and successfully stopped.[36]

Protecting networks in both the governmental and private sectors will require new legislation and regulations. New government agencies may need to be created to help draft specific requirements and to ensure that defense mechanisms are implemented. The US Cyber Command and Israel's National Cyber Bureau are examples of centralized organizations responsible for overseeing the creation and implementation of cyber-defense strategies, including efforts to work with the private sector.

Governments, private companies, and academics should collaborate to develop new defensive technical tools and strategies and to improve existing ones. Governments can offer monetary incentives to private entities, where appropriate, to help build robust defenses[37] Surprisingly simple measures might prove quite effective, such as requiring employees of government agencies and private entities connected to government networks to use strong passwords that are regularly changed, as well as mandatory training to identify and avoid cyberthreats.[38]

Defenders must also consider the supply chain used to design and manufacture their equipment. Hardware, firmware, and software are currently created and built around the world, which makes it difficult to ensure a product is secure. The companies and nations in which such equipment is designed and manufactured may include hidden codes enabling the devices to eventually be hacked. Governments should consider working in conjunction

36 Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

37 Teri Radichel, "Case Study: Critical Controls that Could Have Prevented Target Breach," *SANS Institute*, 2014, https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.

38 Ibid.

with foreign companies and nations to develop an accreditation system that ensures the design and manufacturing processes are transparent.[39] Such a plan does pose dangers, however, particularly in that it might make it more difficult to protect intellectual property, raise the price of the equipment by adding an additional expense, and even stifle the pace of innovation.[40]

The creation of global laws, norms, and international agreements can be useful in bolstering cyber defense. Focusing on protecting critical infrastructure and civilians (for example, banning attacks or intrusions into hospitals) are areas that seem most likely to produce agreement.[41] States should attempt to play an active role in the creation of these laws and norms, as the more involved a state becomes, the greater its ability to protect its interests and shape the future system.[42] Attempting to build laws and norms is an inexpensive undertaking that could potentially improve cybersecurity for nations around the world. If successful they would be a means of bolstering not only defense, but also detection, deterrence, and defeat.[43]

The power of international norms and laws in cyberspace, however, have important limitations. It is unclear how effective international law and norms might be due to the decentralized nature of cyberspace.[44] Furthermore, states might be reluctant to craft agreements regarding uses of the cyber realm that they consider beneficial to their national interests, particularly as this is still a relatively unchartered area.[45] Finally, as noted, it can be difficult to tell when an attack has taken place or to assign attribution, meaning states may believe they can escape punishment.

---

39 David Inserra and Steven Bucci, "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," *Heritage Foundation*, March 6, 2014, http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace.

40 Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

41 Clarke and Knake, *Cyber War*; Sofaer, Clark, and Diffie, "Cyber Security and International Agreements"; Valeriano and Maness, *Cyber War versus Cyber Realities*.

42 Siboni and Assaf, *Guidelines for a National Cyber Strategy*.

43 Observer Research Foundation, "International Public Private Partnership in Cyber Governance (Panel)."

44 Valeriano and Maness, *Cyber War versus Cyber Realities*.

45 Sofaer, Clark, and Diffie, "Cyber Security and International Agreements."

To heighten their ability to defeat attackers in the cyber realm, states can take several steps. They can seek to isolate attacking nations and adopt confrontational tools, such as economic or diplomatic sanctions, in effort to convince them that continued offensive action is too costly. The prospects of defeating an enemy in the cyber realm can be increased if states focus on ways to destroy the opponent's cyber capabilities due to the extensive planning and expensive equipment required to launch sophisticated attacks.[46]

In addition to heightened legal punishments, states can take steps to mitigate the threat from individuals. Isolating individual hackers from the broader community upon which they rely—by disrupting their internet connections or sharing information about the hacker that the community might not approve of—would limit their ability to plan or launch an attack.[47] In addition, states can try to convince some hackers to serve as informants, or penetrate the hackers' networks by planting agents within them. These strategies may also be effective against many NSAs whose members rely on similar communities for support. This strategy may pose risks under international (and domestic) law, but the lack of clearly applicable international law on actions in cyberspace lowers the legal risk.

To enhance resilience in the cyber realm, states should seek a diversity of equipment. Hardware and software should not all be supplied from one source or company. Diverse equipment will allow nations to more quickly isolate the problem, switch to a different company's equipment, and resume operations, although this may increase supply-chain risks. When designing networks, features aimed at improving resilience can be built-in to support the recovery process. To help build resilience for the most critical networks, nations can design cyber architecture that offers multiple pathways for controlling systems.[48] Physical overrides should be built-in to ensure other ways of regaining control of critical systems. Railways, for example, can

46 Jonathan Silber, "Cyber Vandalism – Not Warfare," *Ynet*, January 26, 2012, http://www.ynetnews.com/articles/0,7340,L-4181069,00.html.

47 Scott D. Applegate, "The Principle of Maneuver in Cyber Operation*s,"* in *Fourth International Conference on Cyber Conflict,* ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Talinn: NATO CCD COE, 2012), https://ccdcoe.org/publications/2012proceedings/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf.

48 US Department of Defense, "The DoD Cyber Strategy."

be constructed with the ability to stop a hijacked train by using physical controls that do not depend on cyber systems.

Conclusion

Cyberattacks are not fundamentally different from other threats and can be addressed by applying the classic principles of military strategy, the "four Ds," along with the concept of resilience. These principles may not provide a complete response—much as they do not when applied to other asymmetric and conventional threats—and modifications will certainly be required for the challenges posed by cyberthreats. In those areas in which they prove deficient, however, we are confident that new capabilities will be developed over time as has always been the case when new threats arise.

Research and development are key to the effort to develop these new capabilities across all four Ds and the r. Advanced states have largely managed to ensure that their defense mechanisms have outpaced the offensive capabilities of NSAs. There is, however, no inherent reason this will remain the case, particularly if states fail to take the threat seriously.

This article is a first holistic effort to apply the "four big Ds and a little r'" model to cyberthreats, with the objective of turning it into a conceptual framework that could guide state cyber strategies. Use of the basic framework allows for the development of more detailed plans designed to address the specific demands posed by cyberthreats. The article found that improved intelligence, more resilient cyber architecture, and heightened cooperation both internationally and between the government and private sector are central means for implementing the "four Ds." Further research can help determine additional ways in which the model can be applied or expanded to the cyber realm.