Powering the DIME: Unlearned Lessons of Asymmetric National Power in Cyberspace

Dr. Michael Klipstein
Dr. Pablo Breuer

The United States (US) has a long history of proportional and in-kind response to adversary aggressions. If a US aircraft is shot down, the US will bomb anti-aircraft emplacements and runways or attain air superiority by clearing the skies of other fighter aircraft. If hostile actions are committed in cyberspace, the US will respond with limited cyberspace actions in an attempt to restrain escalation to a kinetic conflict. The US has failed to learn the lesson that conflict in the cyber age is inherently asymmetric and that cyber attack responses need not be quid-pro-quo. There is a range of diplomatic, economic, and information options for effective responses that follows the international legal principle of proportionality and do not necessarily result in escalation to the kinetic actions of warfare. The US should use, and be willing to target in others, all the DIME instruments of national power – i.e., diplomacy, information, military, and economic[1] - to respond to and prevent future aggressions in cyberspace.

Information Flows and Defense of Democracy

There is a vital relationship between information and democracy. In order for a democracy to survive, citizens need valid information to make informed judgments. As Hamilton noted over 200 years ago in the Federalist papers, citizens of a democracy must be educated.[2] They need to have a substantiated and shared understanding supporting the legitimacy of their elections and their government, in addition to a reasonable expectation of economic security.[3] With these foundations in place, a democracy can use contested political knowledge to identify, understand, debate, and solve problems. Conversely, autocratic governments require a monopoly on common political information to keep the system opaque and their citizens under control.

Dr. Michael Klipstein has worked on national cyber topics for over a decade, ranging from USCYBERCOM continuity of government networks, the National Security Agency hard targets, leading a Cyber National Mission Team, and building two Nation Cyber Protection Teams. Later, he created curricula for the Joint Staff for international partner nations in cyberspace, and was a Director of International Cybersecurity Policy for the National Security Council.

Information flow and mass communications remain fundamental to a healthy modern and internetted democracy. If the majority—or even a significant minority—of citizens do not share a common acceptance of elections, legitimacy, economic fairness, and government, democracy is threatened. Likewise, if there are not enough common objectives and some sense of cohesion, the citizens cannot achieve effective pluralities or majorities that underpin policy, and chaos will follow. Conversely, if there is not enough contested information because, for example, government officials allow access only to their interpretation of facts, then citizens do not have access to the marketplace of ideas, debate, and economic innovation. This can lead to tyranny. Examples include government control of information in numerous regimes, and the Kim Family Regime in North Korea isolating the population from outside ideas to forestall rebellion. Democracy depends on the unhindered flow of information balanced between commonly accepted and contested interpretations.

Among the world's consolidated democracies, the US is particularly vulnerable to attacks that affect the free flow and accuracy of electronically exchanged information. First and foremost, very few countries rely on cyberspace as much as the US. Vast portions of national critical infrastructure in the US are connected to the open Internet. Attacks in and through cyberspace are inherently asymmetric in nature. There are simply more critical cyberspace capabilities that the US must defend than there are for adversaries. Further, the capabilities the US must defend are generally more critical to national security than those its adversaries must defend. Finally, unlike many adversaries, much of the US critical infrastructure is commercial; adversaries typically nationalize critical infrastructure and therefore, can more easily enforce both cooperation and compliance.

In today's world, new forms of disinformation present an urgent national threat to the health of our

Dr. Pablo Breuer is a non-resident senior fellow of the Atlantic Council's GeoTech Center and twenty-two-year veteran of the U.S. Navy with tours including military director of U.S. Special Operations Command Donovan Group and senior military advisor and innovation officer to SOFWERX, the National Security Agency, and U.S. Cyber Command as well as being the Director of C4 at U.S. Naval Forces Central Command. He is a DoD Cyber Cup and Defcon Black Badge winner and has been on the faculty at the Naval Postgraduate School, National University, California State University Monterey Bay, as well as a Visiting Scientist at Carnegie Mellon CERT/SEI. Pablo is also a co-founder of the Cognitive Security Collaborative and coauthor of the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework.

democracy-sustaining information environment. The US is at a distinct disadvantage if it limits responses largely to military-borne cyber operations and excludes the other DIME tools – i.e., information, economics, and diplomacy. For example, in a competition limited only to the cyberspace domain, it is likely that the US has more critical capabilities to lose than its adversaries. These capabilities are not limited to just physical critical infrastructure, but include the fundamental underpinnings of our democratic way of life. Conversely, authoritarian adversaries already controlling their internal communications structures can more readily tolerate major losses of access to the free and open internet to protect their critical infrastructure, as well as preventing the significant loss of connected infrastructure.

Only by fully employing its DIME capabilities can the US learn how to bolster its international support and deter adversary nations from conducting offensive cyberspace actions.

DIME Tools of National Power - D

Diplomacy is the domain of the Department of State. Through discussions and agreement of international norms of accepted behavior in cyberspace, the US can lead the world diplomatically. When the US announces a meeting, other states want a seat at the table. This latent power was most recently needed when the 2017 United Nations Group of Governmental Experts on cyberspace failed to reach a consensus on international norms.[4] Increased adoption of norms of acceptable behavior would enable more clearly defined activities. With such norms established—including a consensus on prohibited targets and activities such as masquerading as other nations or launching critical infrastructure attacks leading to civilian deaths—states could better act without ambiguity or fear of argument over whether their actions are a transgression. Similarly, they will benefit from a common understanding of which activities—like espionage—are allowable.

If better equipped, staffed, and authorized to do so, the Department of State then could more effectively, frequently, and likely more persuasively use existing interagency coordination mechanisms to 'demarche' (protest) the attack and the attacker. A good example is the demarche associated with the 2019 Russian attack on Georgian television networks.[5] This "naming and shaming" via demarche in a public forum notifies the global community of the actions and the potential remediation, and it shapes the information environment. Importantly, it also allows the US to build international leverage by partnering with the affected nation for remediation, training, or multilateral response. More is needed to capitalize on the potential of cyber diplomacy: "*The United States should regain the initiative in strategic cyber competition. The Department of Defense has pivoted to a more assertive posture, but the State Department's pivot has just begun.*"[6]

DIME Tools of National Power - I

Adroitly orchestrating the Information tool of the DIME is crucial to effective governmental responses to adversary cyber campaigns. Evidence collected and shared to support the claim that an attack occurred and attribute the attack or campaign to an attacker helps undermine the inevitable denials or counterclaims and misrepresentation of facts by the attacker or its proxies. As the world's nations increasingly rely on a smoothly functioning global internet for commerce, communications, and critical resource supplies, the public revelations of these attacks and their sources has slowly begun to shape the perspectives of states previously resisting attribution to any state, let alone China or Russia. Identifying states clearly shown to threaten the functions of these global information flows can, depending on the circumstances, coalesce sentiment against those states. For example, the 2013 release of the unclassified APT-1 report by the commercial cyber firm Mandiant provided public and substantial evidence of Chinese cyber operations against the US that enabled its leaders to counter PRC denials of having conducted such offensive military action.[7]

In cyberspace, attacks are increasingly less likely to be isolated events, and more likely to be parts of wide-ranging campaigns with larger economic or national security implications. The 2020 Russian SolarWinds attack exemplifies what Russian General of the Army Valery Gerasimov identified in 2013 as the principles operationalizing for the information age the 1990s anti-US Primakov doctrine. Now clearly stated, the Russian state intends to achieve its national objectives through cyberspace and information operations, intertwining conventional and asymmetric means in a whole-of-government, all domains, and permanent conflict between peace and war.[8] As the authoritarian adversaries to democracy have grown into their many and far-reaching cyber campaigns over the past decade, calls among the targeted democracies have led to cooperative cyber defense agreements and training with the US. In providing persuasive information to reveal the adversaries' campaigns and to encourage cooperative support, the US can measurably enhance the effectiveness of its own cyber defense.

DIME Tools of National Power - M

Global militaries now recognize cyberspace as an operational domain with the ability to hold adversaries at risk without firing shots, deploying forces, or launching hostile kinetic actions. Military actions here may include taking control of hard and soft information resources within the adversary's territory, interfering with understanding or effective execution of military or other sectoral movements, or even manipulating the sentiment of population segments to turn against the ruling regime. "*The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. … All this is supplemented by military means of a concealed character.*"[9] Early to engage across domains, the military of Russia, led by its intelligence unit – the GRU,[10] has been deeply involved in cyber-attacks on the US and Europe, as has the Chinese People's Liberation Army – the PLA, most recently through its Strategic Support Forces.[11]

Conversely, in the not-distant past, the Department of Defense would conduct cyber training and online operations with only a select few nations. This was due primarily to a lack of statutory authority to train partner nations in cyberspace activities. Since 2018, the Department of Defense now has had greater autonomy to operate in response to threats and, now with the passage of the 2021 National Defense Authorization Act, and through modification of Section 333 of Title 10,[12] it has the authority to train foreign nations in both defensive and offensive cyberspace operations. This expansion of mil-to-mil cyber coalitions similarly expands the options for national cyber defenses beyond more traditional military operations and the narrower scope of the early cyber era in the 2010s. This now-allowed activity sets conditions to partner with and train less capable nations and build partnerships and alliances, furthering US influence globally.

DIME Tools of National Power - E

Economically, nations are reliant upon the internet for commerce. In 2018, the Council of Economic Advisors conservatively estimated in a 2018 report that malicious cyber activity cost the US economy between $57 billion and $109 billion.[13] This number greatly expands when considering the economic impacts from malicious cyber activity online. Over the course of 2020, cybercrime globally increased to levels never seen before. The average loss from a data breach in the US reached $9 million dollars. Losses from IP theft and ransomware attacks included lost market value, downtime, and reduced productivity.[14]

The economic value and vulnerabilities of the global transport sector are a particular case of lessons yet to be learned and national power yet to be appropriately employed. The 2020 National Maritime Cybersecurity Plan cites numerous examples of the reliance and interconnectedness of nations in cyberspace that extends to their economic dependence on shipping. Non-cyberspace disruptions, such as the recent blockage of the Suez Canal, stopped as much as 30% of the world's container shipping daily resulting in an estimated $400 million each hour

of blockage, along with disruption of supply chains. To illuminate the scale of the backlog, 421 cargo ships had to wait to transit the canal; the largest of these has the capacity to carry 24,000 20-foot containers.[15] If a cyber-attack could precipitate a blockage of the canal, significant damage to global commerce would occur. Similarly, a cyber-attack on the Panama Canal could significantly delay the US from shifting military power, as well as commerce, between oceans. The loss of the Panama Canal would result in increasing the voyage between New York and Los Angeles by over 7,000 miles. Critical maritime supply chains are equally vulnerable to cyber losses and disruptions, as are land systems.[16]

One would expect this economic reality both to alert national domestic action and to elevate attention to the economic tools of national power. Nations cooperatively seeking to improve cybersecurity of often overlooked systems, such as critical infrastructure, would in principle greatly improve economic resilience in cyberspace and reduce the potential monetary cost of malicious cyber activity. However, the lessons of national power and cyber defense in economic terms are at best variably understood. China has demonstrated repeatedly its grasp of the national value of economic warcraft such as its IP theft policy of "rob, replicate, and replace,"[17] pushing victimized firms out of their own markets, and its oft-used economic bribery or blackmail policies against other nations whose citizens displease Chinese leaders.[18]

The US still lacks a comprehensive plan to secure its critical infrastructure with an anchor organization able to implement a cybersecurity strategy nationally, and has yet to create a coordinated and effective use of its economic power for overall cyber defense. The last tool in DIME is, for the cyber era, one of the least well developed.

Putting the Whole DIME Back in the Game

Continued symmetric actions in an asymmetric space leaves the US at a distinct disadvantage. Adversaries seek advantages through manipulation of the internet and its connected activities and potentially strike at the soft underbelly of open societies in an ever-connected world. Unable to reconstruct the internet for security, the US must use all resources and instruments of power to deter adversaries from meddling in information systems in the private and public sectors. By combining Diplomacy, Information, Military, and Economic actions in response to or in advance of attacks, and while the US is still the leading power in the world in all four elements, the US is well-placed to be more effective, efficient, and resilient in deterring adversaries while also strengthening partnerships and alliances among like-minded nations. But the lessons have to be learned, the tools employed, and the policies needed to act recognized clearly and refined smartly. There is not much time left.

NOTES

1. T. Kodalle et al., "A General Theory of Influence in a DIME/PMESII/ASCOP/IRC2 Model," *Journal of Information Warfare* 19, no. 2 (2020).
2. Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers* (Yale University Press, 2009).
3. Henry Farrell and Bruce Schneier, Common-Knowledge Attacks on Democracy (October 2018), Berkman Klein Center Research Publication No. 2018-7, available at SSRN: https://ssrn.com/abstract=3273111 or http://dx.doi.org/10.2139/ssrn.3273111.
4. Arun Sukunmar (July 4, 2017),T*he UN GGE Failed. Is International Law in Cyberspace Doomed as Well?* Retrieved April 2, 2021 from https://www.lawfareblog.com/un-gge-failed-international-law0cyberspace-doomed-well.
5. J. Rudnitsky, N. Chrysoloras, and H. Bedwell, February 20, 2020, Russia Blamed for *'Paralyzing'* Georgia Cyber Attack in 2019, retrieved April 2, 2021 from https://www.bloomberg.com/news/articles/2020-02-20/russia-blamed-for-georgia-cyber-attack-that-raises-sanction-risk.
6. Emily O. Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy (Fall 2020)," *Texas National Security Review* (2020), https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/.
7. APT Mandiant, *APT1 Report: Exposing One of China's Cyber Espionage Units* (February 2013) http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf: Mandiant Ltd, February 13 2013.
8 Eugene Rumer, T*he Primakov (Not Gerasimov) Doctrine in Action - the Return of Global Russia,* Carnegie Endowment for International Peace (June 5, 2019), https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.
9. Molly McKew, September/ October 2017, *The Gerasimov Doctrine*, retrieved April 2, 2021, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.
10. Lilly Bilyana and Joe Cheravitch, "The past, present, and future of Russia's Cyber strategy and forces," paper presented at the 2020 12th International Conference on Cyber Conflict (CyCon, Talinn, Estonia, https://ieeexplore.ieee.org/abstract/document/9131723).
11. Elsa B. Kania and John K. Costello, "The strategic support force and the future of chinese information operations," The *Cyber Defense Review* 3, no. 1 (Spring 2018), https://cyberdefensereview.army.mil/Portals/6/Documents/CDR_V3N1_SPRG2018_Complete.pdf?ver=2018-05-02-141744-830.
12. 2021 National Defense Authorization Act, Section 1201, retrieved April 2, 2021, https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf.
13. Executive Office of the President, "Council of Economic Advisers Report: The Cost of Malicious Cyber Activity to the U.S. Economy," *https://publicintelligence.net/us-malicious-cyber-activity-cost/*, February 2018, https://publicintelligence.net/us-malicious-cyber-activity-cost/, accessed August 2020.
14. Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of CyberCrime,* CSIS and McAfee (2020), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
15. Aaron Clark, Cindy Wang, Ann Koh, and Verity Ratcliffe, 2021, "The Suez Canal Blockage Is Over. Time to Add Up the Damages." https://gcaptain.com/blocked-suez-canal-cost-economy/.
16. Eric de Bodt, Jean-Gabriel Cousin, and Marion Dupire-Declerck, "The CSR Supply Chain Risk Management Hypothesis Evidence from the Suez Canal Ever Given Obstruction," available at SSRN 3867169 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3867169.
17. Smith and Lostri, *The Hidden Costs of CyberCrime.*
18. Simon Sharwood, "Chinese database detailing 2.4 million influential people, their kids, their addresses, and how to press their buttons revealed - Compiling using open source intel [and 10-20 percent not open source] hailed as showing extent of China's surveillance activities [Shenzhen Zhenhua company, China]," *The Register online*, September 15 2020, https://www.theregister.com/2020/09/15/china_shenzhen_zhenhua_database/.