Journal of Cybersecurity, 3(1), 2017, 1–5
doi: 10.1093/cybsec/tyx002
Advance Access Publication Date: 2 March 2017
Editorial

Introduction to the special issue on strategic dimensions of offensive cyber operations

Nations around the world recognize cybersecurity as a critical issue for public policy. They are concerned that their adversaries could conduct cyberattacks against their interests—damaging their military forces, their economies, and their political processes. Thus, their cybersecurity efforts have been devoted largely to protecting important information technology systems and networks against such attacks. Recognizing this point, the Oxford Dictionaries added in 2013 a new word to its lexicon—it defined cybersecurity as "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this."

But a nation can also conduct cyberattacks against other nations as deliberate instruments of policy, and many nations around the world are also exploring the use of offensive cyber operations in such a manner. In the USA, such operations have become increasingly prominent in US policy. For example:

- The deployment and use of Stuxnet against Iranian centrifuges is widely credited with complicating Iranian progress toward a nuclear weapon.[1]
- Presidential Policy Directive 20 (PPD-20), which established US policy for cyber operations, both offensive and defensive, was leaked by Edward Snowden in 2013.[2] According to the Guardian's reporting on PPD-20, offensive cyber capabilities can be used broadly to advance "U.S. national objectives around the world."
- The Department of Defense (DOD) Cyber Strategy [8] (released in April 2015) focuses on "building capabilities for effective cybersecurity and cyber operations to . . . support operational and contingency plans [as one of three objectives]."
- In a speech given at Stanford University releasing the April 2015 cyber strategy, Secretary of Defense Ashton Carter noted that one mission of the DOD is "to provide offensive cyber options that, if directed by the President, can augment our other military systems" [9].
- Today, DOD publicly acknowledges using cyber weapons in its fight against the Islamic State (ISIL). For example, in February 2016, Secretary of Defense Carter said that US Cyber Command is conducting offensive cyber operations to cause ISIL to "lose confidence in their networks, to overload their networks so that they can't function, and do all of these things that will interrupt their ability to command and control forces"[10]. At the same time, he also noted that Cyber Command "was devised specifically to make the United States proficient and powerful in this tool of war." In April 2016, Deputy Secretary of Defense Robert Work said regarding ISIL, "We are dropping cyber bombs. We have never done that before," and "Just like we have an air campaign, I want to have a cyber campaign" [11].

To date, academics and analysts have paid much more attention to cyber defense than to cyber offense. One important reason underlying this imbalance is a high degree of classification about nearly every aspect of US offensive cyber capabilities. Indeed, Michael Hayden, former director of both the NSA and CIA, has noted that as recently as the early 2000s, even the phrase "offensive cyber operations" was classified. Not what it might mean, or what the targets would be, or what technologies would be involved—merely the phrase itself.

High levels of classification and excessive secrecy are especially problematic when policy makers try to understand a new domain of conflict because secrecy inhibits learning across traditional boundaries and new types of conflict necessarily require learning across traditional boundaries. Again, quoting Michael Hayden,

> [d]eveloping policy for cyberops is hampered by excessive secrecy (even for an intelligence veteran). I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones). And the habitual secrecy of the intelligence services bled over into cyberops in a way that has retarded the development – or at least the policy integration – of digital combat power. It is difficult to develop consensus views on things that are largely unknown or only rarely discussed by a select few. [12]

Over the years, a few scholars have ventured into the realm of strategy and doctrine around offensive cyber operations without access to classified materials, but the vast majority has found it easier to stay away from the subject matter entirely. The result is a deep loss for strategic thought, and a stark contrast from the roles that

[1] See, e.g. [1, 2]. According to Albright *et al.* [3], Stuxnet delayed the Iranian nuclear program by about a year.

[2] The leaked PPD-20 can be read in full at: https://fas.org/irp/offdocs/ppd/ppd-20.pdf. PPD-20 has also been the subject of several news articles and editorials, including [4–7] . Because those with clearances are allowed to read press stories reporting on leaked classified documents but not to read these documents themselves outside of cleared facilities, references to PPD-20 in this introduction should be understood as being derived from these articles and not from the original document. In addition, papers in this collection written by individuals who have had proper access to classified cyber-related documents have passed through DOD security review; these papers contain no references to PPD-20, and no individuals with security clearances had any input into this introduction.

non-government researchers played in developing nuclear strategy during the Cold War.[3]

For example, Bernard Brodie developed the fundamentals of deterrence by threat of retaliation as an essential underpinning for nuclear strategy [14] and also the importance of a secure second-strike capability (i.e. deliverable nuclear weapons that could survive a first strike by an adversary) for strategic stability [15]. Herman Kahn introduced the key strategic notion of an escalation ladder as it might apply across the entire range of quite limited conventional conflict to all-out nuclear conflict [16]. Thomas Schelling developed influential theories for promoting arms control involving strategic nuclear weapons [17].

In March 2016, a two-day research workshop was held at Stanford University on offensive cyber operations. Supported by the Lakeside Foundation and the Hoover Institution and organized by the Cyber Policy Program at Stanford University in consultation with US Cyber Command, the workshop brought together a number of distinguished researchers from academia and think tanks as well as current and former policy makers in the Defense Department and US Intelligence Community. All discussions and papers were unclassified. The papers appearing in this special issue represent a selection of the contributions to the workshop. Papers appearing here have been greatly revised and peer-reviewed according to the standards of the journal.

The workshop focused on strategic dimensions of offensive cyber operations, which can be used across a wide range of scenarios and for a wide range of purposes. Tactical uses of a weapon (cyber or otherwise) focus on short-term, narrow goals—how to defeat the adversary in the next village tomorrow. Strategic uses of weapons, by contrast, focus on longer term, more overarching goals and are designed to affect the broader dynamics between potential adversaries both on and off the hot battlefield.

A definitional note: for purposes of this workshop, offensive cyber operations were conceptualized as the use of cyber capabilities for national security purposes intended to compromise the confidentiality, integrity, or availability of adversary information technology systems or networks; devices controlled by these systems or networks; or information resident in or passing through these systems or networks. In general as well as for this workshop, offensive cyber operations include those that compromise confidentiality ("cyber exploitation") and those that compromise integrity or availability ("cyberattack").

A good place to start thinking about offensive cyber operations in a strategic context is to consider some of the unique characteristics of weapons in cyberspace that bear on national security.

- In cyberspace, instruments used to gather intelligence and attack (i.e. to cause damage) are difficult to distinguish. Because the same techniques are usually used to gain access to adversary systems and networks for intelligence gathering and for causing harm, an adversary that detects a penetration cannot be certain of the penetrator's intent—and, therefore, may misperceive an attempted intelligence operation (a cyber exploitation) as an attack.
- Offensive cyber operations act most directly on intangibles—information, knowledge, and confidence. To be sure, cyber operations can cause tangible effects, as when the information in question is integral to the operation of devices or equipment that affect the physical world. But offensive cyber operations are fundamentally deceptive in nature—at a tactical level, no cyberattack tells the user of a computer "click on this link and your computer will be compromised by a malicious adversary." Human cognition is, of course, based on the availability of information—and if the humans involved doubt the provenance of the information available to them, their concerns may well prompt them to assume the worst.
- To a degree unprecedented with kinetic weapons, the effectiveness of a cyber weapon is a very strong function of the target's characteristics. The nature of target–weapon interaction for kinetic weapons can usually be estimated on the basis of physics-based experimentation and calculation. Not so with cyber weapons and their targets, where the smallest change in configuration of the target can, under many circumstances, completely negate the effectiveness of a cyber weapon against it. Consequently, intelligence information on target characteristics must usually be obtainable in large volume, be of high quality, and be available at the time of the weapon's use.
- Advance preparation of a cyber target may be required for an attack to be successful. For example, it may be necessary to surreptitiously install a "back door" that will grant the attacker access at a later time for downloading a customized attack payload that takes into account new intelligence information that may then become available.

These characteristics appear in the three interrelated themes explored by the seven papers in this special issue: cyber strategy and doctrine for offensive use of cyber weapons; operational considerations in using cyber weapons; and escalation dynamics and deterrence. (A fourth workshop theme—the role and relationship of the private sector to offensive cyber operations—is not reflected in this special issue.)

Cyber strategy and doctrine

The DOD Cyber Strategy specifically states that the USA will respond to cyberattacks against its interests "at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law." Henry Farrell and Charles L. Glaser ("The Role of Effects, Saliencies and Norms in U.S. Cyberwar Doctrine") consider how the USA should choose between cyber and kinetic responses to cyberattacks. Their starting premise is that decisions about deterrence and warfighting should be based on the effect a given US attack will have, not the means by which that effect is produced. But, they note, perceptions matter as well—adversaries may perceive different forms of retaliation that do equal damage as differently punishing and differently escalatory, and in particular, that kinetically caused damage is perceived as "more serious" than comparable damage caused by a cyberattack. If so, the role of kinetic retaliation for deterring and responding to cyberattacks may well be less than it otherwise would be.

Operational and tactical considerations

Operational considerations are implicated in the strategic use of weapons in that they speak directly to how military forces are employed to gain military advantages over an adversary and thereby attain strategic goals. Such considerations focus on the design, organization, and conduct of major operations and in-theater campaigns. Of course, the borderless nature of cyberspace makes the

[3] The points made in this paragraph and additional discussion of the deleterious effects of overclassification regarding offensive cyber operations can be found in Lin and Grossman [13].

definition of "in-theater" problematic, a point suggesting that offensive cyber operations are themselves likely to be conducted without regard for national borders.

An operation plan is a complete and detailed plan for military operations that would be executed upon receipt of appropriate orders for particular military contingencies. In "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," Austin Long uses the frame of nuclear planning processes to understand how strategic targeting using cyber weapons might occur, considering how the organizational processes used to plan for the use of nuclear weapons and to execute such plans could in fact be applied to cyber weapons as well. It is noteworthy that according to the Guardian [4], PPD-20 calls for the identification of "potential targets of national importance" where offensive cyber capabilities "can offer a favorable balance of effectiveness and risk as compared with other instruments of national power." Identification of such targets is analogous to the development of a target list for the Single Integrated Operating Plan for using strategic nuclear weapons, today known as OPLAN 8010, "Strategic Deterrence and Global Strike."

In "Second Acts in Cyberspace," Martin Libicki considers the connection between tactics and the conduct of an extended cyber campaign. He notes that adversaries are likely to adapt as we conduct offensive cyber operations against them. Such adaptations could occur relatively quickly and may reduce the effectiveness of subsequent operations unless the initial operations are crafted carefully to minimize adversary opportunities to adapt.

Escalation dynamics

Escalation dynamics and deterrence refer to processes by which conflict can start, how smaller conflicts can grow into bigger ones, and how these processes can be interrupted to make the outbreak or escalation of conflict less likely. Intelligence collection—one of the primary functions of certain types of offensive cyber operations—can be problematic from the standpoint of limiting escalation. Consider, for example, the sensitivity of nations to the security of their nuclear capabilities, regarded as the ultimate guarantor of their security against hostilities from other nations. Gathering intelligence can provide reassurance about the putative intent of an adversary. But because it is often unclear in the initial stages of an offensive cyber operation whether such an operation is intended to gather intelligence or to prepare the cyber battlefield and that offensive cyber operations are likely to be used early in a conflict,[4] cyber-enabled intelligence collection directed against nuclear command and control facilities—especially if noticed by an adversary during a crisis—may be misinterpreted as a sign that a preemptive attack is imminent.

In "Thermonuclear Cyberwar" Erik Gartzke and Jon Lindsay raise another important question regarding escalation dynamics. Noting that cyber capabilities depend on concealing information about cyber vulnerabilities from the other side, they argue that if the latter has nuclear capabilities, its confidence in its ability of use those capabilities may be excessively high, and that they will be less likely to back down in a crisis—thus increasing the likelihood that nuclear or conventional war will break out.

In "Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes," Michael Gross, Daphna Canetti, and Dana Vashdi focus on the psychological harm and consequential impact of offensive cyber operations on public confidence in important national institutions. They observe in experiments that in the face of hostile cyber activity, many citizens reevaluate their confidence in public institutions and increase their support for harsh military responses, tendencies that may well increase public pressures for cyber or even kinetic escalation.

One important factor that might cause unintended escalation of a conflict is the use of a weapon that causes more damage than was intended by the attacker. Steven M. Bellovin, Susan Landau, and Herbert Lin point out in "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications" that with appropriate intelligence in hand, cyberattacks can be designed and conducted in a way that limits damage to the intended targets: discriminating cyber weapons are technically possible. The article also addresses technical means for limiting the proliferation of cyber weapons that could otherwise occur, a factor that can work to mitigate the security dilemma in cyberspace.

A second factor in unintended cyber escalation is an inappropriate scope and nature of the rules of engagement for the use of cyber weapons. A foundational rule of engagement for offensive cyber operations appears to be articulated in PPD-20.[5] According to public news reports,[6] PPD-20 directs that cyber operations "reasonably likely to result in significant consequences require *specific presidential approval*" (emphasis added), where "significant consequences" are known to include loss of life, serious levels of retaliation, damage to property, adverse foreign policy consequences, or economic impact on the country.

In addition, both PPD-20 and the DOD Cyber Strategy note that offensive cyber operations must be conducted in accordance with the laws of armed conflict (LOAC), just as all other US military operations are conducted. To address issues of collateral damage, the DOD has established "No-Strike and the Collateral Damage Estimation Methodology" [19] that requires commanders to compile a list of "No-Strike Entities" upon which kinetic or non-kinetic attacks would violate LOAC. Public reports also indicate that PPD-20 directs officials to weigh "the potential threat from adversary reactions" and "the risk of retaliation," both considerations in managing risks of escalation. Such considerations would help to shape the establishment of a Restricted Target List, which involve valid military targets but which for non-LOAC considerations such as escalation should not be attacked in certain specified ways. Mission-specific rules of engagement (also known as supplementary rules of engagement) account for No-Strike Entities and Restricted Targets.

In "Rules of Engagement for Cyberspace Operations: A View from the United States," C. Robert Kehler, Herbert Lin, and Michael Sulmeyer provide an overview of how the DOD generally conceptualizes such rules of engagement, but without reference to PPD-20. They note that the US military seeks as much as possible to integrate cyber weapons into its operational tool kit within a common framework of principles that apply to all weapons, and from the DOD perspective, principles that inform rules of engagement for traditional kinetic weapons can and do inform rules of engagement

[4] See e.g. [18].

[5] As this issue is going to press, a new administration in the USA has just taken office and emphasized, at least rhetorically, the importance of going on the offensive in cyberspace. Whether and how, if at all, this new emphasis will change the current rules of engagement framework for cyber weapons is uncertain at this time.

[6] See e.g. [4, 5]. All references to PPD-20 in this introduction are based on these public news reports and not on any classified document that may have been leaked into the public domain.

that govern cyberspace operations as well. Nevertheless, several characteristics of operations in cyberspace and the use of cyber capabilities complicate the formulation of cyber-specific rules of engagement, including the borderless geography and range of effects possible on the Internet, ambiguity of adversary intent arising from the difficulty of distinguishing between intelligence-gathering for reconnaissance and preparation for attack, and difficulties of attribution in cyberspace. A paucity of historical experience with cyber operations in a military context will hamper the formulation of rules of engagement for cyber weapons; consequently, special efforts should be made to impart experience (such as might be developed through war gaming and tabletop exercises) to the appropriate leaders and commanders.

It is only within the last few years that the US Department of Defense has designated cyberspace as a domain of conflict. Many policy makers are struggling today with how best to integrate offensive cyber capabilities with other instruments of military and national power. The papers presented at this workshop demonstrated that thinking about offensive cyber operations as instruments of national policy need not require *de novo* construction. Indeed, many of the questions and issues that attend to the strategic dimensions of offensive cyber operations arise in other kinds of military operations. Because the cyber domain is unlike other domains of conflict in important ways, it is not surprising that some of the answers and responses to these questions and issues in the cyber domain are different. More clearly delineating what's new and what isn't when it comes to offensive cyber operations is an important step forward.

The increasing prominence of offensive cyber operations as instruments of national policy warrants serious research conducted by independent scholars at universities and think tanks in the same way that a great deal of such research has been conducted on various defense-related topics such as missile defense, nuclear strategy, naval operations, and so on. Such research contribute to the overall body of useful knowledge on which policy makers can draw, and even if a given research-based idea does not immediately have policy significance, research adds to the inventory of parts that may be useful to policy in the future. In other words, such work helps to "prepare the terrain for future consideration of policy options—… loosening the intellectual bolts on issues that are not quite ready for public consideration" [20].

This workshop was convened in large part to demonstrate the realistic possibility of collaboration between government policy makers and independent non-government researchers working on strategic dimensions of offensive cyber operations on an unclassified basis. The workshop organizers believe that the publication of these papers in this special issue is proof that this demonstration was successful.

Herbert Lin
Stanford University

Amy Zegart
Stanford University

Acknowledgments

The organizers of the workshop (Lin and Zegart) extend their gratitude to the editors at the *Journal of Cybersecurity*, specifically Tyler Moore and David Pym (editors-in-chief), Susan Landau and Brandon Valeriano (area editors who managed the peer-review process for papers related to policy). Neither Susan Landau nor Herbert Lin were involved in any editorial decisions regarding papers in this volume for which either was a coauthor.

References

1. Broad W, Markoff J, and Sanger D. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (21 January 2017, date last accessed).
2. Warrick J. "Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack." http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html (21 January 2017, date last accessed).
3. Albright D, Brannan P, Stricker A *et al. Preventing Iran from Getting Nuclear Weapons: Constraining Its Future Nuclear Options. Institute for Science and International Security*, 2012. http://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf (21 January 2017, date last accessed).
4. Greenwald G, MacAskill E. "Obama orders US to draw up overseas target list for cyber attacks." http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (21 January 2017, date last accessed).
5. Editorial Board. "Cyberwar: The White House is thinking ahead." https://www.washingtonpost.com/opinions/cyberwar-the-white-house-is-thinking-ahead/2013/06/16/b4a0ab00-d4fa-11e2-a73e-826d299ff459_story.html (21 January 2017, date last accessed).
6. Gertz B. "Cyber War Details Revealed - Secret presidential order reveals policies for waging offensive, defensive cyber warfare." http://freebeacon.com/national-security/cyber-war-details-revealed/ (21 January 2017, date last accessed).
7. Clayton M. "Presidential cyberwar directive gives Pentagon long-awaited marching orders." http://www.csmonitor.com/USA/Military/2013/0610/Presidential-cyberwar-directive-gives-Pentagon-long-awaited-marching-orders-video (21 January 2017, date last accessed).
8. Department of Defense. "The DOD Cyber Strategy." http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21 January 2017, date last accessed).
9. Carter A. Remarks by Secretary Carter at the Drell Lecture, Cemex Auditorium, Stanford Graduate School of Business, Stanford, California. http://www.defense.gov/News/News-Transcripts/Transcript-View/Article/607043 (5 April 2016, date last accessed).
10. Lyngaas S. "Carter: U.S. disrupting Islamic State computer networks." https://fcw.com/articles/2016/02/29/carter-isis-networks.aspx (21 January 2017, date last accessed).
11. Browne R, Starr B. "Top Pentagon official: 'Right now it sucks' to be ISIS." http://www.cnn.com/2016/04/13/politics/robert-work-cyber-bombs-isis-sucks/ (21 January 2017, date last accessed).
12. Hayden MV. The making of America's cyberweapons. *Christian Science Monitor*, 24 February 2016.
13. Lin H, Grossman T. The practical impact of classification regarding offensive cyber operations. In: Harrison, R, Herr, T (eds.), *Cyber Insecurity: Navigating the Perils of the Next Information Age*. New York: Rowman & Littlefield, 2016, 313–27.
14. Brodie B. *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt, Brace and Company, 1946.

15. Brodie B. *Strategy in the Missile Age*. Washington, DC: RAND Corporation, 1959.
16. Kahn H. *On Escalation: Metaphors and Scenarios*. Piscataway, NJ: Transaction Publishers, 1965.
17. Schelling TC, Halperin M. *Strategy and Arms Control*. New York: Twentieth Century Fund, 1961.
18. Lin H. Reflections on the new DOD Cyber Strategy: what it says, what it doesn't say. *GJIA*, March 2017 (forthcoming).
19. Chairman of the Joint Chiefs of Staff Instruction. "No-Strike and the Collateral Damage Estimation Methodology [CJCSI 3160.01A]." https://info.publicintelligence.net/CJCS-Collateral Damage.pdf (21 January 2017, date last accessed).
20. DelRosso S. Activating the power of ideas. *Carnegie Rep* 2014; **7**: 3–5.