STRATEGIC STUDIES QUARTERLY

The Convergence of Information Warfare

Martin C. Libicki

Abstract

If information technology trends continue and, more importantly, if other countries begin to exploit these trends, the US focus on defeating a cyberwar threat will have to evolve into a focus on defeating a broader information warfare threat. It is far less plausible to imagine a cyber attack campaign unaccompanied by other elements of information warfare—in large part because almost all situations where cyber attacks are useful are those which offer no good reason not to use other elements of information warfare. Thus the various elements of information warfare should increasingly be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations.

✳ ✳ ✳ ✳ ✳

In the 1990s, information warfare (IW) burst on the scene and subsequently left with a whimper. It came to prominence when a community of military strategists, citing the works of John Boyd, the Tofflers, and Sun Tzu, argued that competition over information would be the high ground of warfare.[1] In this struggle, some would collect ever-more pieces of information ISR (intelligence, surveillance, and reconnaissance) systems. Others would use the tools of electronic warfare (EW), psychological operations (PSYOP), and cyber operations to degrade what the other side knew or could control. Many felt there had to be a unified theory of information warfare out there to integrate these various elements.

Information warfare receded when people realized there was no such unified theory and hence no good reason to organize militaries as if there were.[2] The ISR community kept building and operating systems of greater acuity and range. Electronic warriors went back to mastering their magic in support of air operations, counter–improvised explosive

Martin C. Libicki is the Maryellen and Dick Keyser Distinguished Visiting Professor at the US Naval Academy's Center for Cybersecurity Studies and author of *Cyberspace in Peace and War*. His research has focused on the impact of information technology on domestic and national security. Previously, he worked for RAND (where he is still adjunct), the National Defense University, and the Navy staff. He holds a master's degree and a PhD from the University of California–Berkeley.

devices, and other combat specialties. Psychological operators continued to refine the arts of persuasion and apply them to an increasing roster of disparate groups. Cyber warriors bounced through the space community before getting their own subunified command within which they could practice their craft. This refusal to coalesce happened for good reason. Although the *ends* of each of these separate activities—to gain the information advantage—were similar, the *means* by which these separate activities were carried out were very different. Expertise in sensors, emitters, content, and code (for ISR, EW, PSYOPs, and cyber operations, respectively) hardly resembled one another. Each called for different equipment and training; there was scant reason for them to be organized together.

However, given today's circumstances, in contrast to those that existed when information warfare was first mooted, the various elements of IW should now increasingly be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations. This claim is supported by three emerging circumstances. First, the various elements can use many of the same techniques, starting with the subversion of computers, systems, and networks, to allow them to work. Second, as a partial result of the first circumstance, the strategic aspects of these elements are converging. This makes it more likely that in circumstances where one element of IW can be used, other elements can also be used. Hence, they can be used together. Third, as a partial result of the second circumstance, countries—notably Russia, but, to a lesser extent, North Korea, Iran, and China—are starting to combine IW elements, with each element used as part of a broader whole.

Taken together, these emerging circumstances create challenging implications for the future of US information warfare. Simply put: if information technology trends continue and, more importantly, if other countries begin to exploit these trends, then as a general rule, the US focus on defeating a cyberwar threat will have to evolve into a focus on defeating a broader IW threat. Perceptions of cyberwar will likely need rethinking. One could debate plausibility of a determined cyber attack campaign unaccompanied by physical violence and destruction. It is becoming far less plausible to imagine a cyber attack campaign unaccompanied by other elements of information warfare. Preparations to retain resilience and accelerate recovery after a cyber attack campaign

would also do well to address the complications that could arise if other IW elements were used in conjunction with such cyber attacks.

Computer Subversion as Information Warfare

Subversion can be the starting point for multiple IW elements. The point of subversion is to usurp the normal state in which systems do only what their owners want. Instead, they do things hackers want. In some cases hackers can get systems to react to inputs in unexpected ways, and in other cases such systems can execute an arbitrary set of commands provided by hackers.

Once hackers compromise a system they have many options. These days the most common is to collect information. When national intelligence agencies do this, it is called cyber espionage, a subset of intelligence collection. Whereas human intelligence takes place one person at a time, cyber espionage can take place millions of records at a time. A prime example is the Office of Personnel Management (OPM) hack—22 million personnel records were stolen. It showed how one side's voluminous data keeping can be another side's intelligence mother lode. It can be a lot easier to find those who collect information and steal from them than it is to collect the information afresh. The advantage of piggybacking can be applied to the many ways that individual data are generated, with the theft of information already ordered in databases (as with OPM) as the clearest case of leveraging the other side's work. Indeed, imagine what could be done with the Chinese database of political "creditworthiness."[3] But there are other targets, notably the large compilations created via web transactions and surveillance systems.[4] For overhead images, consider the burgeoning market for gyrocopters or other types of unmanned aerial vehicles; for ground imagery, there are cell phone snaps—which could wind up in an intelligence database by being donated, posted, offered, aggregated, and handed over—or simply stolen. If the Internet of Things evolves as it appears to be doing, homes could leak information from sources almost too many to keep track of.[5] Again, why collect what can be stolen?

In many cases, the purpose of stealing all the haystacks is to find the few needles of particular interest. But one can also make hay with such information. Once collected, data-mining techniques permit analyses and exquisite tailoring of such information.[6] The ability to build increasingly realistic simulations of individuals, indeed perhaps of most

of a population, could arise from integrating data streams with enormous cloud-based storage, powerful processing, and a dash of artificial intelligence. Such simulations may be used to test every individual's reaction to events (both virtual and real), advertising, political campaigns, and psychological operations and even to guess what might go viral through person-to-person interactions.

One way to use information on individuals gathered through a combination of ISR (albeit often third-party ISR) and cyber operations is through exquisite psychological operations, messages tailored to one person at a time. The trend to "micro-appeals" is already obvious in US domestic political campaigns and advertising.[7] As long as psychological operators grasp the essentials of the cultures of those they wish to influence, there is every reason to believe that a data-mining campaign to characterize individuals precisely can help in crafting the message most likely to resonate with them. The messages do not have to convince (e.g., buy this, believe that); in a conflict context, their point may be to induce fear or at least anxiety and thus paralyze resistance one person at a time; tailoring messages to each person erodes the solidarity enjoyed by groups all facing the same threat. Doxing individuals—which is posting the results of hacking to embarrass or blacken their reputation through randomly found (as in the Ashley-Madison hack) or deliberately selected (as in the Democratic National Committee hack) information—is increasingly common.

Cyber operations can enhance PSYOPs in other ways. Devices and websites both can be infected to introduce users to propaganda that shows up in unexpected places or carries unexpected credentials.[8] Compromising systems can also aid psychological operations by directing people to sites they had not intended to go or to sites that falsely purport to be where they had intended to go. Similar techniques can and are being used to enhance the credibility and page rankings of favored sites. Spam-bots can be engineered to dominate online debates.[9] Troves of material stolen from political opponents can be seasoned with concocted documents with appropriate levels of verisimilitude.[10] Overall, the shift from more-curated mass media to less-curated Internet websites and uncurated social media permits outright falsehoods to spread much faster and farther.

Other harvests from compromised systems—notably the other side's—are the classic ones of disruption, corruption, and, possibly, destruction.

Websites can be knocked offline when computers (and, one day, kitchen appliances?) of web users are converted into bots and herded into botnets. To date, the damage from all cyber attacks combined (as distinct from cyber espionage) has been modest, but it is an open question whether the threat will stay contained. Can increasingly sophisticated defenders withstand assaults from increasingly sophisticated attackers? How much will growing digitization and networking increase a country's attack surface?

The Internet of Things is another new playground for hackers, which could harm not only such things but also whatever they could come into contact with. To date, it has been difficult for hackers to hurt people and break things, in large part because the major industrial facilities, having seen others attacked through cyberspace, are taking information security more seriously. But most of the Internet of Things will be owned by people unable or unwilling to pay requisite attention to security; many of those who build these networked things seem to have ignored the security lessons that information system makers have painfully learned. Many of the things that are becoming networked (notably, cars and drones) are capable of causing serious harm to their owners and worse, third parties, if their controls are usurped. Even if wholesale chaos is unlikely, there will be new ways of heightening anxiety or targeting individuals from afar.[11]

To a partial extent, electronic warfare can also be carried out by controlling devices that emit radio-frequency (RF) energy. New forms of RF signals pervade homes and cities: Bluetooth, Wi-Fi, 5G, keyless entry systems, and Global Positioning System (GPS), to name a few. The coming Internet of Things is essentially an Internet of RF-connected items. If software-defined radios (those capable of broadcasting or receiving signals over an arbitrarily selected frequency) become ubiquitous, they could be hijacked to jam or spoof targets hitherto inaccessible using traditional EW boxes.[12]

In sum, systems compromise is becoming a core technique across all IW elements. It remains the key element of cyber attack. Cyber espionage itself is a growing element in ISR. Subverting sensors or the data repository allows harvesting of surveillance collected by others. Similar subversion can allow data collection at such high resolution as to permit individuals to be simulated; this knowledge permits PSYOPs to be optimized; compromising media creates new conduits for persuasion

or the manipulation of fear. Hijacking the Internet of Things can create new ways to create physical harm. Finally, some forms of EW can be carried out by subverting RF-transmitting devices. Opportunities abound.

IW in the Niche of Cyberwar

The second basis for arguing that the various elements of information warfare should be considered parts of a greater whole results from four propositions. First, cyberspace operations differ in key respects from kinetic operations. Second, other elements of IW differ from kinetic operations in similar ways. Consequently, third, these various elements can all be used for operations where these characteristics are important or even essential (or where opposing characteristics make using kinetic operations impractical or unwise). And, fourth, for such operations, the use of IW elements should therefore be considered together rather than separately. Consider that the first two positive propositions now ground the last two propositions (what is versus what could or should be).

Several broad characteristics differentiate cyber from kinetic operations: the variance of their effects, their nonlethality, their ambiguity, and the persistence of the war-fighting community. Take each in turn.

Higher degrees of variance are more likely to characterize cyber attacks than kinetic attacks. Most cyber attacks cause temporary or at least reversible effects whose extent depends on the technical details of the target systems (many of which change in ways attackers cannot expect), the services such systems provide (often opaque to attackers), how such services are used (also opaque), and how quickly the attacked system can be restored (often unclear even to defenders, much less attackers). Outcomes can easily vary from expectations in such an environment. Even estimating battle damage assesment, not to mention collateral damage, can be unreliable particularly if defenders isolate an attacked system from the rest of the world to restore it. Because systems have to be penetrated before they are attacked, the timing of success in going after hard targets is often unpredictable (with Stuxnet, for instance, effects had to await some unknown person inserting a USB device into a computer inside the closed network).

Insofar as other IW operations start with compromising systems, they consequently would wait until those systems are sufficiently compromised; thus these IW operations can also start with large degrees of unpredictability. But even after this unpredictability is taken into

account, the IW effects are, to a further extent, unpredictable. PSYOPs, for instance, entail persuasion in that one hears echoes of retail tycoon John Wanamaker: "Half the money I spend on advertising is wasted; the trouble is I don't know which half." Unpredictability is higher if leveraging social media rather than mass media, because the former depends on the willingness of those receiving the message to pass it on and thus have it go viral. Although EW and ISR have features that allow predictability, their ultimate effectiveness often depends on the tricks the other side has or lacks: do war fighters know what frequency-protection measures are being used; will spoofing be successful or will the other side see through some tricks; how well does the other side camouflage itself, hide itself, or use denial and deception techniques? Even if one side sees what it sees (or thinks it sees) it can only guess at what it cannot see.

One obviously different effect is the general nonlethality of information operations vis-à-vis kinetic operations. Rarely do cyber attacks in particular or other IW techniques in general create casualties. After nearly a quarter-century of alarm over the lethality of cyber attacks, no one has yet been hurt in a cyber attack, and there are only two known occasions of serious physical destruction (Stuxnet and a blast furnace in Germany).[13] EW is even more benign (electronics can be fried, but this generally requires either close range or nuclear effects). This has several implications. IW can rarely disarm (even if it can temporarily disable equipment or at least discourage its use) or make others realistically fear for their lives. It can be used in circumstances where causing casualties may yield condemnation or beget an overreaction.

Ambiguity entails doubt over who is doing what and for what purpose. Cyberspace operations unfold in a dense fog of ambiguity (even as certain fogs that have bedeviled kinetic operations are lifting). In the wake of a cyber attack, although context may provide a strong clue of who did what, attribution can be a problem if and when attackers take pains to mask their involvement. Adding ambiguity to IW means that the global reach of the Internet widens the number of potential attackers because small states and nonstate actors can threaten large ones. It does not take a large state apparatus to hack computers or devices, exploit borrowed ISR, or generate propaganda—although it does take clever people to do this well. Countries can use IW elements to harass countries they cannot hope to touch in traditional kinetic ways—as long as they aim for societal effects rather than those requiring kinetic follow-up

(e.g., that would exploit the other side's confusion when its information turns to mush).

In some cases even the effects may be less than obvious (e.g., a subtle intermittent corruption of data), particularly if the attack is halted midway. Discovering a penetration into a system does not indicate whether its purpose was to spy on or to interfere with a system and, if the latter, when the system would go awry—if the penetration is discovered, which often takes months or years if it takes place at all. Thus intentions cannot always be inferred from actions, and indications and warnings have yet to be terribly useful[14]; there are, for example, few if any steps that must precede a cyber attack by x hours and whose discovery can be used to predict when a cyber attack is coming. Inasmuch as cyber attack techniques are unlikely to work if their particulars are exposed, these particulars are deep secrets. No one really knows what others can do in cyberspace. Few show what they themselves can do; past attacks may be demonstrative but not necessarily repeatable—hence they are better indicators of what was rather than what will be.

Other IW elements would be colored by such ambiguity if they worked by first subverting systems. To the extent that the source of such subversion was not obvious, then neither would be the identification of what element of information warfare (e.g., surveillance, messaging, manipulating RF emissions) was the purpose. Similarly, to the extent that the purpose of such subversion was not obvious, it complicates drawing inferences once such subversion is discovered.

But again, many information warfare elements would have ambiguous features even if carried out through non-cyber means. It can be hard to locate the source of a transmitter that moves and broadcasts infrequently. People often do not know they are under surveillance or even if they do, from where and using what means. And even if these are known, the use to which such information is put can be little better than a guess. The origins of a meme or a rumor circulating within social media can be easily obscured. The ultimate target of surveillance, emission, or disinformation may not be the proximate one.

Finally, information warriors—notably cyber warriors—may persist longer than their kinetic counterparts because they work as small units or even individuals without expensive, bulky, or otherwise telltale equipment. Information warriors rarely need be in harm's way nor need their operations have any obvious signature that distinguishes them from

civilians. Their ability to generate instant worldwide effects from anywhere gives them plenty of places to hide in relative safety. Thus it is hard to put them out of commission by attacks (and certainly not by cyber attacks). Because hacking looks like typing it can escape casual oversight. Because their efforts need little specialized equipment, hackers may even survive their country's demise. This latter characteristic does not extend to forms of IW that use expensive organic assets like aircraft-mounted jamming pods, surveillance satellites, or mass media outlets. But a force that can no longer count on such assets may be able to leverage subverted systems to make up some of what these assets supplied. Such a force can persist in fighting even if dispersed.

Implications of Variance, Nonlethality, Ambiguity, and Persistence

These characteristics of information war shape how countries might want to use (and not use) information warfare. Take each characteristic in turn.

Variance complicates the use of IW elements to support modern kinetic combat or various forms of irregular warfare, all of which represent a highly complex and synchronized affair dependent on the careful integration of effects. On such battlefields, IW is used almost entirely in support of kinetic operations. Although militaries favor efforts with high degrees of effectiveness, many, perhaps most, military operations are predicated on the finite and bounded success of discrete, well-defined support efforts (e.g., radars are jammed to permit aircraft to reach a target and return home safely). While exceeding objectives is nice, it is usually not worth the risk of *not* meeting objectives. So although IW elements may be included in operational plans, they are more likely to be nice-to-have but not need-to-have tools—apart from traditional and more predictable (i.e., measurable and discrete) aspects of EW or ISR. Conversely, unpredictability matters less if IW is the main event where the point is to achieve an agglomeration of effects so that overachievement in one endeavor can compensate for underachievement in another, particularly if done to support strategic narratives that shape decisions or actions. There is a big difference between (1) needing A to work in order that B would work and (2) knowing that if A and B both work they reinforce the message that each other is sending. Arguably, cumulative rather than

coordinated effects are what better characterize the use of IW against societies in comparison to its use against militaries.

In any event, civilian targets are softer targets for IW than are their military counterparts. Civilian systems are less well protected and are more often exposed to outside networks. Civilians rarely practice operational security. Security is still an afterthought for the Internet of Things. Civilian RF signals rarely use antijamming or antispoofing techniques. Civilians themselves are often softer targets than war fighters, who are trained to be inured to most IW. So IW is likely to have a different target than kinetic warfare.

Nonlethality and ambiguity, for their part, may be exploited to modulate the risk of reprisals—notably, violent reprisals—for having carried out information operations. Information warriors may well doubt that target countries will mount a kinetic response, which can break things and kill people, to an IW campaign that does neither. Indeed, it is unclear whether countries would mount a kinetic response to an information warfare campaign that happens to wreak some damage and hurts a few people. Similarly, there is little precedent for responding to propaganda with force.

If the target cannot be sure who is causing its suffering it may have to forego both disarming and deterring the attacker. Even if the target later concludes that it knows who is doing what or at least cannot afford to remain passive (doubts notwithstanding), it may not be able to do so easily. Having accepted continued harassment as the new normal puts the onus on the defender to risk escalation to end harassment; it has to shift from deterrence to the much harder art of compulsion.

Nevertheless, an IW campaign that wants to avoid triggering a violent reaction from the target requires knowing where the latter's thresholds lie[15]—and it may have little better than a guess to work with. The true threshold will depend on personalities, politics, and foreign pressure. Injury may be, alternatively, likened to a boiling frog (leading to underreaction) or the straw that broke the camel's back (leading to an unexpected reaction). An attack that passes notice may be only subtly different from one that excites retaliation. The target state may deem something put at risk to be more sensitive than outsiders realize even as it assumes that its own sensitivities are known and understood by others. The threshold may also vary by information war element. Cyberwar can levy large costs (it may take $1 billion to replace South Korea's national identification

system[16]) without anything actually breaking. Broad foreign surveillance can be scary without much cost in life and property, but it can also be shrugged off. EW, however, can interfere with transportation operations by making them unsafe, but if there is damage, fingers may point to those who choose to operate in the face of risks.[17]

These days, countries appear to be mindful that there are limits. Although Russia took territory, tried to interfere with Ukrainian elections, and disrupted Ukraine's parliamentary sites with a distributed denial-of-service (DDOS) attack, it has refrained from all-out cyber attack or EW against civilian targets and is not trying to foment disorder in core Ukrainian areas, which may now be out of reach for Russia. It probably does not want Ukraine to feel under existential threat unless and until Ukraine reacts forcefully to Russian incursions.

Persistence means that IW can be hard to disable even as kinetic forces are being targeted for destruction. Much as ambiguity makes it hard to figure out if information warfare has started, persistence means that the end itself may not be declared unless someone concedes and perhaps not even then—persistence can be a two-edged sword for a country that turns such tools on but cannot credibly promise to turn them off. President Kennedy's phrase "a long twilight struggle" may become apropos when discussing information warfare.[18] Indeed, were the Cold War to have taken place in the modern era, its day-to-day activities may well have included many such elements.

In many ways, we have already seen this kind of war before: terrorism combines high levels of variance (many would-be terrorist attempts fail or are thwarted), modest levels of lethality compared to historic kinetic warfare, ambiguity (particularly as regards state sponsorship), and persistence. If terrorism remains the "propaganda of the deed" (as anarchists argued in the nineteenth century), then its link to IW is clearer. Because full-fledged IW requires, as a target, a well-digitized society, one might view it as terrorism against the rich.

Commingling IW Elements

The third reason to take the convergence of IW seriously is because the Russians and others are doing so in theory and in practice (i.e., Ukraine). Russia's "hybrid warfare" campaign features an admixture of specialized units (*speznats* and artillery), logistical support of local insurgents—and copious amounts of IW. The latter has included DDOS attacks on Ukrainian

sites, an attack on Ukraine's power grid, near-successful attempts to corrupt Ukrainian election reporting, heavy electronic warfare in combat areas, the severing of electronic links between Ukraine and Crimea, the physical destruction of communications links, and heavy amounts of propaganda directed at Russian-speaking Ukrainians among others.[19] Russian cyber espionage against Western targets appears to have grown; they are certainly being detected more often. Examples include NATO and the unclassified e-mail systems of the White House, the US State Department, the Joint Chiefs of Staff, the Democratic National Committee, and the German Parliament.

Russian theory underlies its practice. As security specialist Keir Giles has observed, "the Russian definition [is] all-encompassing, and not limited to wartime . . . [and] much broader than simply sowing lies and denial, for instance maintaining that Russian troops and equipment are not where they plainly are. Instead, Russian state and non-state actors have exploited history, culture, language, nationalism and more to carry out cyber-enhanced disinformation campaigns with much wider objectives."[20] Others note that, "Cyberspace is a primary theater of Russia's asymmetrical activity . . . because . . . [it] offers a way to easily combine fighting arenas, including espionage, information operations, and conventional combat, and to do so behind a curtain of plausible deniability."[21] Russian military doctrine argues, "military dangers and threats have gradually shifted into the information space and internal sphere of the Russian Federation . . . [requiring military forces to] create conditions, that will reduce the risks that information and communication technologies will be used [by others] to achieve military-political goals . . . ."[22] Russia expert Dmitry Adamsky argues, "It is difficult to overemphasize the role that Russian official doctrine attributes to . . . informational struggle in modern conflicts . . . [which] comprises both technological and psychological components designed to manipulate the adversary's picture of reality, misinform it, and . . . forces the adversary to act according to a false picture of reality in a predictable way. . . . Moral-psychological suppression and manipulation of social consciousness aim to make the population cease resistance, even supporting the attacker, due to . . . disillusionment and discontent."[23]

Similar beliefs may motivate North Korea, which has carried out cyber attacks against South Korea, notably its banks, media companies, and national identification system. It also engages in intermittent electronic

warfare (GPS jamming directed at passing aircraft[24]) and directs propaganda south (which the South Korean government takes seriously enough to censor). China for its part has pressed on with a more tactical approach to IW; in late 2015 it merged its integrated network electronic warfare activities with its space and ISR activities.

Russians and to a lesser extent others believe that IW should be approached holistically for two reasons. First, IW should not be dismissed out of hand—and Russia seems satisfied that it worked in Ukraine. Second, to the extent that the United States has to contend with Russian operations, it helps to grasp how IW elements fit together.

The Future of US Information Warfare

Given the trends and convergence of information warfare, how might the United States exploit these trends? On the face of it, no country is better positioned to carry out information war. US skills at cyberwar have no equal. US institutions lead the world in the commercialized arts of persuasion, and the collection and analysis of personal information for commercial and political purposes have proceeded farther in the United States than anywhere else. No country is more advanced in digitizing and networking things. US expertise in systems integration is unchallenged. But figuring out how to effectively harass another country's citizens one at a time does not seem like an urgent or important, much less permissible, US national security problem to solve.

Nevertheless, because other countries are interested in figuring out how to combine these elements of information warfare into a unified whole, the United States ought to understand how to do so itself. First, there may be useful techniques learned even if the larger idea is unacceptable. Second, even though the prospect of operating a harassment campaign based on IW is unpalatable, one cannot rule out occasions in which the only way to stop others from doing so (short of armed conflict) may be a credible offensive capability. Third, just as the Defense Advanced Research Projects Agency was established shortly after *Sputnik* launched for the purposes of preventing surprise—and then went ahead to develop technology that surprised others—dabbling in the arts of IW could help prevent external developments from surprising the United States.

If the United States were to embed cyber operations within a broader context of IW, then the mission and organization of US Cyber Command would have to change. Today it boggles the mind to ask an organization

(deservedly) wrapped in great secrecy to take the lead for influence operations, which are ineluctably public. But in time, the choice to overlook the psychological effects of cyber operations or the potential synergy between psychological operations and cyber operations would make just as little sense.[25] Serious thought may be needed on how to build an information warfare authority, whether housed under one organization or achieved through intense coordination among the various communities: cyber warriors, cyber intelligence collectors, electronic warriors, psychological operators, and, in some cases, special operators.

Perceptions of cyberwar might also need rethinking. One could debate the plausibility of a determined cyber attack campaign unaccompanied by violence. However, it is harder to imagine a cyber attack campaign unaccompanied by other elements of information warfare, in large part because almost all situations where cyber attacks are useful are also those which offer no good reason not to use other elements of IW. For instance, if another country is trying to exhaust US will by conducting cyber attacks on information systems that underlie US commerce, they would not necessarily try to blow up trucks. Rather, cyber attacks that compromise trucks, to reduce confidence in their safe operation, are more plausible, if achievable. It is also quite likely that in a systematic campaign, attackers would try to jam GPS or override satellite uplinks, using cyber espionage to create the impression that they are watching Americans and are prepared to dox particular individuals, or letting a thousand trolls bloom to create a news environment that would pit Americans against each other. The latter activities have attributes of nonlethality, unpredictability, ambiguity, and persistence that allow them to fit the strategic niche occupied by cyber attacks. Preparations to retain resilience and accelerate recovery after a cyber attack campaign would also do well to address the complications that could arise if other elements of IW were used in conjunction with cyber attacks.

Against such a campaign how should countries respond? The terms war and warfare suggest a military response, and one cannot completely rule out circumstances in which the only way to reduce suffering from an IW campaign to within reasonable levels is to threaten force. But many characteristics of IW—nonlethality, ambiguity, and persistence—suggest using the same mind-set, tools, and rules used against crime. Much crime fighting involves changing the environment. The moral environment affects an individual's propensity to join a fight; it includes

ethical norms and the social influences that arise when communities alternatively applaud, excuse, or shun criminals. The physical environment can also be changed. Cyber attacks can be countered by cybersecurity standards, air-gapping (e.g., isolating controls from the grid), and information sharing (making it as mandatory as accident investigations). EW threats may be mitigated through spectrum and transmission-device controls (which make it easier to identify attacking devices). ISR exploitation may be frustrated by policies such as restricting unmanned aerial vehicles, surveillance cameras, data collection, and data retention (so that there is less data to steal). Ultimately it has been the evolution of the information economy that has provided the means by which hostile others can run a pervasive harassment campaign. There is little evidence that others have been willing to invest enough time and trouble to make a comprehensive campaign work and no evidence yet that such a campaign could work, in the sense of shifting the balance of power among various actors. But it would not hurt to ask to what extent the collection and connection of personal information in modern economies provide more raw material than they should for someone else's hostile IW campaign.

Even if defeating information warfare through conventional war is unrealistic, the prospect of managing it down to tolerable levels need not be. Treating IW like crime rather than state acts shows a refusal to accept it as "acceptable" behavior but does not signal a commitment to violence as an appropriate response. Such a strategy requires a narrative that calls on the public for both less and more: less in that conscious mobilization is deliberately eschewed and more in that managing such a conflict may require fundamental and lasting changes in how people go about their daily lives. SSQ

Notes

1. John Boyd's briefing "Winning and Losing" exists only in summary form. For more on his work, see, for instance, Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (London: Routledge, 2006); Alvin and Heidi Toffler, *War and Anti-War, Survival at the Dawn of the 21st Century* (New York: Little Brown and Co., 1993); and Sun Tzu, *The Art of War*, trans. Thomas Cleary (Boston: Shambhala Publications, 2005).

2. The author's contribution to this process is *What Is Information Warfare?* (Washington, DC: National Defense University Press), 1995.

3. Celia Hatton, "China 'Social Credit': Beijing Sets Up Huge System," *BBC*, 26 October 2015, http://www.bbc.com/news/world-asia-china-34592186. FireEye's William Glass observed that "a centralized system would be both vulnerable and immensely attractive to hackers. 'There is a big market for this stuff, and as soon as this system sets up, there is great incentive for cybercriminals and even state-backed actors to go in, whether to steal information or even to alter it.' " Simon Denyer, "China's Plan to Organize Its Society Relies on 'Big Data' to Rate Everyone," *Washington Post*, 22 October 2016, https://www.washingtonpost.com/world/asia_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd_story.html.

4. Ludwig Siegele, "The Signal and the Noise," *Economist*, 26 March 2016, 10, http://www.economist.com/news/special-report/21695198-ever-easier-communications-and-ever-growing-data-mountains-are-transforming-politics. "Facebook and Google . . . know much more about people than any official agency does and hold all this information in one virtual place. It may not be in their commercial interest to use that knowledge to influence political outcomes, as some people fear, but they certainly have the wherewithal."

5. Law Enforcement Cyber Center, "Internet of Things Infographic," accessed 8 December 2016, http://www.iacpcybercenter.org/officers/iot/.

6. Adm Michael Rogers, National Security Agency director, has opined that the Office of Personnel Management attack is a signal of what may become an emerging trend in network attacks by other nation states: because of the proliferation of tools that can readily perform detailed analytics on large data sets, adversaries will increasingly seek to purloin entire haystacks of data all at once and search for the needles later. *See* Jared Serbu, "Cyber Command Chief Frustrated by Lack of Industry Participation," Federal News Radio, 8 July 2015, http://federalnewsradio.com/cybersecurity/2015/07/cyber-command-chief-frustrated-lack-industry-participation-u-s-tries-build-early-warning-system-cyber-attacks.

7. "Ted Cruz Took a Position on Iowa Firework Sales to Try and Sway 60 Voters," The Week, 2 February 2016, http://theweek.com/speedreads/603059/ted-cruz-took-position-iowa-firework-sales-try-sway-60-voters.

8. Apparently, so can airport public address systems. *See* "The Alleged Chinese Hacking at Vietnam's Airports Shows That the South China Sea Battle Isn't Just in the Water," *Huffington Post*, 6 August 2016, http://www.huffingtonpost.com/helen_clark/china-hack-vietnam-south-china-sea_b_11357330.html.

9. Siegele, "The Signal and the Noise," 9. "During the Maidan protests in Ukraine in 2013–2014, Russian 'spam bots' had a much larger presence in Ukraine's Twittersphere than tweets by the Russian political opposition."

10. Cory Bennett, "Democrats' New Warning: Leaks Could Include Russian Lies," 17 August 2016, http://www.politico.com/story/2016/08/democrats-cyberhack-russia-lies-227080.

11. What may be highly implausible *in toto* is not necessary implausible considered one incident at a time; see, for instance, Reeves Wiedeman, "The Big Hack," *New York Magazine*, 19 June 2016, http://nymag.com/daily/intelligencer/2016/06/the-hack-that-could-take-down-nyc.html.

12. Inasmuch as traffic lights are normally accessible only through wired connections and Bluetooth devices, they might seem immune to mass remote hacking—until the population of infected Bluetooth devices crosses some threshold to where nearly every control box is within range of some such device.

13. Several major cyber attacks, most notably at Saudi Aramco and Sony, have rendered computers inoperable, but that was as a result of hard-to-reverse changes in software, not damaged hardware.

14. The FBI supposedly warned the Democratic National Committee (DNC) that their systems could be hacked but not with enough specificity to do anything much about it; see Even Perez, "Sources: US Officials Warned DNC of Hack Months before the Party Acted," CNN, 26 July 2016, http://www.cnn.com/2016/07/25/politics/democratic-convention-dnc-emails-russia/.

15. The concept of "gray zone" is one specifically below the threshold of conventional conflict; see, for instance, Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: US Army War College Strategic Studies Institute, 2 December 2015), http://strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1303.

16. Iain Thomson, "South Korea Faces $1bn Bill after Hackers Raid National ID Database," *The Register,* 14 October 2014, http://www.theregister.co.uk/2014/10/14/south_korea_national_identity_system_hacked/.

17. Mary-Ann Russon, "Russia Blamed for Crashing Swedish Air Traffic Control to Test Electronic Warfare Capabilities," *International Business Times*, 14 April 2016, http://www.ibtimes.co.uk/russia-blamed-bringing-down-swedish-air-traffic-control-test-electronic-warfare-capabilities-1554895.

18. Pres. John F. Kennedy, "Inaugural Address," 20 January 1961, http://www.presidency.ucsb.edu/ws/?pid=8032.

19. "Russia jammed and intercepted Kiev signals and communications, hampering the other side's operations, and effectively detaching the peninsula from Ukraine's information space," quoted from Pasi Eronen, "Russian Hybrid Warfare: How to Confront a New Challenge to the West" (Washington, DC: Foundation for Defense of Democracies, June 6, 2016), 6, 8, http://www.defenddemocracy.org/content/uploads/documents/Russian_Hybrid_Warfare.pdf.

20. Kier Giles, *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, 20 May 2016, 2, http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

21. Margaret Coker and Paul Sonne, "Ukraine: Cyberwar's Hottest Front," *Wall Street Journal*, 10 November 2015, http://www.wsj.com/articles/ukraine-cyber wars-hottestfront-1447121671.

22. *Voyennaya Doctrina Rossiiskoy Federatsii* (2014), rg.ru/2014/12/30/doktrina-dok.html (citation courtesy of Olesya Tkacheva).

23. Dmitry Adamsky, "Cross-Domain Coercion: the Current Russian Art of Strategy," *Proliferation Papers*, no. 54 (November 2015), 26–27, https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

24. Choe Sanghun, "North Korea Tried Jamming GPS Signals across Border, South Korea Says," *New York Times*, 1 April 2016, http://www.nytimes.com/2016/04/02/world/asia/north-korea-jams-gps-signals.html. Although that particular attempt disrupted little, earlier attempts in 2012 had forced incoming aircraft to use alternative navigation methods.

25. The broad psychological ramifications of cyber operations, which this paragraph talks about, should be distinguished from the use of psychology to assist cyber operations by, for instance, enhancing social engineering or understanding how mucking with an adversary's command-and-control systems will change how its forces are commanded.

Disclaimer