Security Studies
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fsst20

Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace

Erik Gartzke & Jon R. Lindsay
Published online: 22 Jun 2015.

To cite this article: Erik Gartzke & Jon R. Lindsay (2015) Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace, Security Studies, 24:2, 316-348, DOI: 10.1080/09636412.2015.1038188

To link to this article: http://dx.doi.org/10.1080/09636412.2015.1038188

Security Studies, 24:316–348, 2015

ISSN: 0963-6412 print / 1556-1852 online
DOI: 10.1080/09636412.2015.1038188

Routledge
Taylor & Francis Group

Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace

ERIK GARTZKE AND JON R. LINDSAY

It is widely believed that cyberspace is offense dominant because of technical characteristics that undermine deterrence and defense. This argument mistakes the ease of deception on the Internet for a categorical ease of attack. As intelligence agencies have long known, deception is a double-edged sword. Covert attackers must exercise restraint against complex targets in order to avoid compromises resulting in mission failure or retaliation. More importantly, defenders can also employ deceptive concealment and ruses to confuse or ensnare aggressors. Indeed, deception can reinvigorate traditional strategies of deterrence and defense against cyber threats, as computer security practitioners have already discovered. The strategy of deception has other important implications: as deterrence became foundational in the nuclear era, deception should rise in prominence in a world that increasingly depends on technology to mediate interaction.

Is offense easier than defense in cyberspace? It is widely believed that societal dependence on the Internet and cheap hacking tools enable nation-states and lone hackers alike to reach across borders, without warning, to access vital computer networks. Once inside, they can pilfer valuable secrets or disable critical equipment. At the same time, the ubiquity, anonymity, and complexity of the Internet are believed to undermine efforts at disarmament, defense, and deterrence. Because cyber aggression exploits the same open channels used for legitimate commerce and communication, offensive techniques cannot simply be prevented or proscribed. If hackers can evade

Erik Gartzke is professor of political science at the University of California, San Diego.
Jon R. Lindsay is assistant professor of digital media and global affairs at the Munk School of Global Affairs, University of Toronto.

detection and disregard threats of retaliation, then deterrence loses its credibility. Coordination failures among firms and government actors, together with the attackers' ability to vary their signatures faster than defenders can detect them, further amplify the costs of network protection. As a result, it has become accepted wisdom that offense dominates defense in the cyber domain.[1]

Why should computer security rely on the electronic equivalent of moats or trench lines for protection? Why, too, should the logic of nuclear deterrence be expected to map in a linear fashion onto cybersecurity? Just as the nuclear revolution led to new modes of strategic interaction, the expansion of computer networks may necessitate reconsideration of security logics. Deterrence was not a new strategy in the 1950s, but it became much more salient and visible as effective defense against nuclear attack appeared impossible. Attending to the broader logic of coercion, the United States and other nations developed deterrence as the bulwark of the new strategic environment rather than as the strategic adjunct it had been previously. Deterrence is rightly recognized as a strategic alternative distinct from defense for protecting the status quo.[2]

Today, the specter of cyber warfare and espionage seems to pose conditions in which the strategies of the past again appear inadequate. This should not be misconstrued to mean that cybersecurity poses anything like the terrors of nuclear war—it does not. Nevertheless, it is reasonable to seek protection against emerging exploitative and force-multiplying digital threats, such as they are. Unfortunately, the widely held and largely unquestioned assumption of offense dominance in cyberspace has discouraged exploration and assessment of ways in which the Internet might actually promote stability. Yet as major technological or even civilizational change generates security challenges, it also creates opportunities. Rapid innovations in mobility, firepower, and targeting in the last century appeared at first to favor the offense (e.g., the blitzkrieg), but these same factors were also valuable to the defense, provided that commanders understood, and were prepared to exploit, the new conditions with elastic combined-arms defenses and deep counterattacks.[3] If denying, deterring, or defending against Internet aggression proves ineffectual when used alone, then considering ways to ensure

[1] Many sources depict cybersecurity as a revolutionary threat including, inter alia, Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010); Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011); Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly, 2012); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (Fall 2013): 7–40.

[2] For a review of the classic deterrence literature, see Lawrence Freedman, *Deterrence* (New York: Polity Press, 2004).

[3] Stephen Biddle, "Rebuilding the Foundations of Offense-Defense Theory," *The Journal of Politics* 63, no. 3 (2001): 741–74.

that the inevitable attacks become fruitless or even harmful to the perpetrator seems appropriate. Deception is just such an approach or strategy, one that has already begun to prove itself critical in the information age.

The telegraph, introduced well over a century ago, enabled instantaneous communication at distance, but it also invited interlopers to tap the wire. Pioneers of military and diplomatic telecommunications quickly realized that there was no way to prevent an enemy from listening in or from jamming or incapacitating their circuits. By the traditional standards of defense, which focused on preventing access by intruders, telegraphy and telephony were a disaster. Fortunately, the inherent vulnerability of electrical communication to eavesdropping or attack was not in itself an insurmountable problem and could even be used to advantage by the target. If one could not prevent the adversary from intercepting or disrupting communications, one could still manipulate what was learned and thus what conclusions opponents were likely to draw from available information. Disguise, disinformation, and other counterintelligence practices came into their own as strategies in the telecommunications era, albeit in shadowy agencies with limited or supporting roles within a broader military and diplomatic apparatus.

Deception as a distinct strategy has become particularly potent with the advent and growth of the Internet, just as deterrence came into its own in the nuclear era.[4] Present for some time in military and intelligence circles, these practices have become both more central and widespread in the Internet era simply because there are so many more opportunities to exploit user trust and design oversights. Cyber attackers rely on deception for almost any offensive advantage, but they do not have a monopoly on duplicity and stealth. Moreover, the strategy of deception is not without risk for an attacker who cannot abide compromise. The same factors that are believed to weaken disarmament, deterrence, and defense also make it possible to lay traps for an adversary online. Offensive and defensive advantages in cyberspace thus result from relative organizational capacity for employing deception and integrating it with broader strategic initiatives, not from categorical features or attributes of Internet technology.

Much of the early scholarly literature on cyber warfare has focused on tamping down the exaggeration common in policy discourse.[5] We seek to

[4] There is surprisingly little research on deception as a strategy in security studies, although uncertainty is critical to warfare. One study argues that deception may be more cost-effective than simple secrecy or honesty; Jun Zhuang, Vicki M. Bier, and Oguzhan Alagoz, "Modeling Secrecy and Deception in a Multiple-Period Attacker–Defender Signaling Game," *European Journal of Operational Research* 203, no. 2 (1 June 2010): 409–18. See also David Ettinger and Philippe Jehiel, "A Theory of Deception," *American Economic Journal: Microeconomics* 2, no. 1 (February 2010): 1–20.

[5] For criticism of cyber-threat inflation, see Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics* 4, no. 1 (2008): 19–36; Evgeny Morozov, "Cyber-Scare: The Exaggerated Fears over Digital

advance the theoretical debate beyond these important correctives by describing ways in which strategic actors can pursue and protect their interests in cyberspace. This article first summarizes the conventional wisdom about offense dominance in the cyber domain and highlights the absence of empirical activity to substantiate this belief. We then argue that the assumption that traditional security strategies are inadequate in the cyber domain is in fact predicated on a more fundamental potential for deception inherent in information technology. Next we explain how deception can also improve protection, first because an attacker's reliance on deception becomes self-limiting and second because defenders can employ strategies of deception as well, as computer security engineers have already begun to recognize. Finally, we bring our argument full circle by pointing out that the salience of cyber deception actually calls into question categorical assumptions about offense dominance, even as the prominence of deception in cyberspace has other implications for the conceptualization and practice of strategic affairs.

THE HACKER WILL ALWAYS GET THROUGH?

Actors seeking to maintain the status quo against revisionist aggression are generally believed to possess three well-known options. First, they can disarm opponents by banning certain weapons or eliminating the threat through preventive or preemptive attack. Second, they can deter their adversaries by threatening unacceptable retaliation if aggressive action is taken. Third, they can defend against active attacks by parrying or absorbing blows.[6] In logical order of application, disarming an opponent makes deterrence and defense unnecessary, and successful deterrence precludes the need for an active defense. However, actors seeking to minimize provocation often apply these strategies in reverse. Defensive measures, if effective and affordable, will often seem the most reliable way to protect valuable interests. Threats associated with deterrence are more risky since they can be misperceived or discounted and because valuable assets are left exposed. Disarmament can

Warfare," *Boston Review* (July/August 2009); Jerry Brito and Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy* (Arlington, VA: George Mason University, Mercatus Center, 2011); Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013); Bruce Schneier, *Liars and Outliers: Enabling the Trust That Society Needs to Thrive* (Indianapolis: Wiley, 2012); Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10, no. 1 (2013): 86–103; Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (Winter 2014): 7–47.

[6] Some strategists distinguish between threats of retaliatory punishment (deterrence by punishment) and threats of an effective defense (deterrence by denial). See Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961). As used in this paper, "deterrence" emphasizes deterrence by punishment, and "defense" refers to the means used to blunt the effectiveness of an attack.

seem more dangerous still because parties to arms treaties can renege, and preventive war may be, in Bismarck's colorful description, "suicide from fear of death." In practice, these strategies are exercised jointly or simultaneously. For instance, criminal law makes burglary illegal, precluding the option of theft for most citizens. At the same time, police enforcement deters potential burglars, and locks and alarms defend against break-ins.

The traditional overlap between security strategies began to unravel in the modern era with technological changes. The advent of nuclear weapons especially necessitated more careful dissection of the independent effects of each strategy. Actors under anarchy could not credibly commit to adhere to arms control agreements that they would prefer to violate in pursuit of a more favorable balance of power. Even if an adversary tried to honor its commitments, civil-military dual-use applications further complicated the effectiveness of monitoring and enforcement.[7] Defense against nuclear weapons, ballistic missiles, and multiple warheads appeared futile, especially if a reserve retaliatory capability (submarines, dispersed missiles, airborne bombers, etc.) could be expected to ride out any attempted disarming counterforce strike. Thus the logic of deterrence—inhabited by the threat of second-strike retaliation—stood out as the most feasible option, even as some sought to resuscitate disarmament or defense to escape the material dangers and psychological discomfort of mutual vulnerability.[8]

The Ubiquity, Anonymity, and Complexity of the Internet

The advent of the Internet has led many to question whether defense has become unhinged and, moreover, whether any strategy can effectively protect the status quo. In an article written during his tenure as US assistant secretary of defense, William J. Lynn III asserts, "In cyberspace, the offense has the upper hand." Unplugging is not an option because "information technology enables almost everything the U.S. military does." Defense cannot be assured because "programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions. In an offense-dominant environment, a fortress mentality will not work. The United States cannot retreat behind

[7] Marc Trachtenberg, "The Past and Future of Arms Control," *Daedalus* 120, no. 1 (Winter 1991): 203–16; Joseph S. Nye Jr., "Arms Control and International Politics," *Daedalus* 120, no. 1 (Winter 1991): 145–65. The record for biological weapons is far from encouraging. See Albert Carnesale and Richard N. Haass, eds., *Superpower Arms Control: Setting the Record Straight* (New York: Harper, 1987); Joseph S. Nye Jr., "Arms Control After the Cold War," *Foreign Affairs* 68, no. 5 (Winter 1989): 42–64; Milton Leitenberg, Raymond A. Zilinskas, and Jens H. Kuhn, *The Soviet Biological Weapons Program: A History* (Cambridge, MA: Harvard University Press, 2012).

[8] The superpowers never stopped pursuing counterforce options during the Cold War. See Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, nos. 1–2 (2014): 38–73.

a Maginot Line of firewalls or it will risk being overrun." Furthermore, traditional deterrence models of assured retaliation falter because "it is difficult and time consuming to identify an attack's perpetrator. Whereas a missile comes with a return address, a computer virus generally does not." Given these unsavory options, Lynn identifies defense (and deterrence by defensive denial) as the least bad option: "Deterrence will necessarily be based more on denying any benefit to attackers than on imposing costs through retaliation. The challenge is to make the defenses effective enough to deny an adversary the benefit of an attack despite the strength of offensive tools in cyberspace."[9]

Disarmament is especially impractical in cyberspace. Commoditized hardware and software components and high-speed networks have enabled tremendous innovation and productivity in nearly every industrial and governmental sector.[10] Aggression is just one more creative application (or "mash up") of the same assets that propels the civil-military dual-use problem to the extreme.[11] The tools needed for many forms of Internet mischief can inexpensively be downloaded, purchased in cybercrime markets, or co-opted from unsuspecting third parties or even the networks of the target entity itself. A computer prevented from accepting connections to the outside world would be rendered safe, but it is also much less useful. Perhaps the greatest obstacle to cyber disarmament treaties emerges from the fact that the very actors that are most threatened by cyber war in one moment benefit from exploitation and espionage in the next.[12]

The problem of cyber deterrence has already spawned a large and diverse literature, with most authors concluding that deterrence is undermined by difficulties in assigning responsibility for ambiguous attacks.[13] Although the attribution problem is probably overstated, identifying attackers is a time-consuming process relying on circumstantial evidence.[14] If victims of attack cannot identify particular assailants, then threats to punish them lose credibility and indiscriminate retaliation is likely to prove counterproductive. Nevertheless, these problems may be surmountable in practice. As the former commander of US Cyber Command, General Keith Alexander, stated in

[9] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* (September/October 2010).

[10] James W. Cortada, *The Digital Hand*, 3 vols. (Oxford; New York: Oxford University Press, 2008).

[11] Jonathan L. Zittrain, "The Generative Internet," *Harvard Law Review* 119, no. 7 (May 2006): 1974–2040.

[12] Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, Koret-Taube Task Force on National Security and Law Future Challenges Essay (Stanford, CA: Hoover Institution, 2011).

[13] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); National Research Council, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010); David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy* 9, no. 5 (September/October 2011): 36–40.

[14] David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks*, 25–40; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–37.

his testimony before Congress, "I can assure you that, in appropriate circumstances and on order from the National Command Authority, we can back up the department's assertion that any actor threatening a crippling cyber attack against the United States would be taking a grave risk."[15]

Still, General William Shelton, commander of US Air Force Space Command, highlights three problems with applying the deterrence framework to cyber attacks: rationality, attribution, and secrecy. "For deterrence to work, adversaries are expected to think and act rationally," Shelton observes, but this might be harder to assume with a wider range of actors with access to cyber tools. Even for rational adversaries, however, the attribution problem diminishes the impact of retaliation because there is no guarantee of finding and harming the culprit. Furthermore, if the deterrent punishment is envisioned as a cyber attack, then signaling becomes even more problematic. Particular cyber capabilities cannot be revealed in advance because they "are disposable assets," as Shelton points out: "You use them once and they're pretty much gone, because once you do it people are very quick, they'll figure it out, and they'll learn how to block it for next time."[16] In other words, a cyber weapon must remain secret in order to work, which of course means that it is not of much use as a vehicle for generating deterrent threats.

Many experts believe that defense (often repackaged as "resilience") is the only available alternative, if still a highly imperfect one. There are too many vulnerabilities and too few resources to protect much, if anything, from the concerted efforts of an adept attacker.[17] Cyber defense must succeed everywhere and every time, many argue, but attackers need only succeed once to compromise a system. Meanwhile, coordination costs among defenders are thought to scale up more quickly than an attacker's costs in finding and hacking a target. Market failures exacerbate technical challenges as vendors prioritize being first to market over investment in security, users avoid patching regularly or practice weak operational security (i.e., cyber hygiene), and actors who generate the greatest risk do not bear proportionate consequences.[18] Government attempts to address market failures can

[15] Quoted in Zachary Fryer-Briggs, "U.S. Military Goes on Cyber Offensive," *Defense News*, 24 March 2012. Alexander's successor, Admiral Michael Rogers, has also testified that deterrence is feasible: "We have the ability to respond proportionately and discriminately in both kinetic and non-kinetic modes when we can meet attribution requirements. . . . I believe there can be effective levels of deterrence despite the challenges of attribution." *Advance Questions for Vice Admiral Michael S. Rogers, USN, Nominee for Commander, United States Cyber Command*, US Senate Committee on Armed Services (11 March 2014) (testimony of Michael Rogers), http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

[16] Quoted in Fryer-Briggs, "U.S. Military Goes on Cyber Offensive."

[17] Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies* 36, no. 1 (2013): 120–24.

[18] Ross Anderson and Tyler Moore, "The Economics of Information Security," *Science* 314, no. 5799 (27 October 2006): 610–13; Johannes M. Bauer and Michel J.G. van Eeten, "Cybersecurity: Stakeholder

make a bad problem worse as law enforcement, intelligence, military, and industrial regulatory agencies struggle to coordinate policy and as activists resist encroachment on civil liberties.[19]

As a result, offense dominance is often represented as an inevitable consequence of information technology. In describing a supposed cyber revolution, Lucas Kello points to the "unpredictability and undetectability" of offense, machines that are "inherently manipulable by pernicious code," the "complex defense surface" of digital systems, the "fragmentation of defense" across private sector firms, and the "supply chain risks" of "off-the-shelf and offshore manufacturers" in order to "underscore the immense disadvantages of defense against cyberattack."[20] This view is consistent with the widely held assumption that technology decisively and systemically determines the offense-defense balance.

Where Are All the Attacks?

If geographic, technological, or organizational conditions make conquest feasible at low cost or risk in comparison with the effort of defending the same objectives, then aggressors should be more tempted to launch an attack, the security dilemma and negative spirals should be more intense, and greater uncertainty and secrecy should lead to more miscalculation and war.[21] According to a prominent body of international relations theory, high levels of offense dominance, in general, should be tied to a heightened risk of war.[22] The deficiencies of traditional protective strategies as summarized above should thus make cyber war the sum of all fears, as many have predicted.

Indeed, the US Department of Defense gets attacked ten million times a day; a US university receives a hundred thousand Chinese attacks per day; and one firm measures three thousand distributed denial of service (DDoS)

Incentives, Externalities, and Policy Options," *Telecommunications Policy* 33, nos. 10–11 (November 2009): 706–19.

[19] The major challenges of cybersecurity are generally acknowledged to be political and economic rather than technological. Oftentimes feasible technological solutions exist, but organizations and individuals lack the incentives to use them properly. See Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. (Indianapolis: Wiley, 2008); Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013).

[20] Kello, "The Meaning of the Cyber Revolution," 27–30.

[21] Charles L Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton, NJ: Princeton University Press, 2010), 117–121.

[22] George H Quester, *Offense and Defense in the International System* (New York: J. Wiley & Sons, 1977); Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214; Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (Spring 1998): 44–82; Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca, NY: Cornell University Press, 1999); Karen Ruth Adams, "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance," *International Security* 28, no. 3 (Winter 2003/4): 45–83.

attacks per day worldwide.[23] In reality, however, most of these so-called attacks are just routine probes by automated networks of compromised computers (botnets) run by profit-seeking criminals or spy bureaucracies—a far cry from terrorism or military assault. The most alarming scenarios of a "digital Pearl Harbor" or "cyber 9/11" have yet to materialize despite decades of warning. The Stuxnet worm caused limited and temporary disruption of Iran's nuclear program in the late 2000s, the only known historical case of infrastructure damage via deliberate cyber attack, but this operation seems to reveal more about the strategic limitations of cyber war than its potency.[24] The cyber revolution should presumably provide rivals with potent new tools of influence, yet actual cyber disputes from 2001 to 2011 remain restrained and regionalized, not disruptive and global.[25] Computer espionage and nuisance cybercrime thrive, to be sure, but they are neither as prevalent nor as costly as they might be, leading skeptics to describe US losses as "a rounding error" in a fifteen trillion dollar economy.[26] It is possible in principle that the same tools used for computer-network exploitation may one day be leveraged for more destructive strikes. Yet even if the nontrivial operational challenges of cyber war can be overcome, proponents of the cyber-revolution thesis have yet to articulate convincing strategic motives for why a state or non-state actor might actually use cyber capabilities effectively.[27] A considerable shortage of evidence in the study of cyber conflict is thus a source both of concern and relief.

That cyber war remains unusual is puzzling in light of the widely held belief that offense is easier than defense in cyberspace. A straightforward implication of the notable scarcity of cyber war would be that, contrary to conventional wisdom, cyberspace is defense dominant for some reason. More carefully stated, since clearly there is much mischief online, offense dominance may exist only for nuisance attacks that are rarely strategically

[23] Fryer-Briggs, "U.S. Military Goes on Cyber Offensive"; Richard Pérez-Peña, "Universities Face a Rising Barrage of Cyberattacks," *New York Times*, 16 July 2013; Arbor Networks, "ATLAS Summary Report: Global Denial of Service," http://atlas.arbor.net/summary/dos (accessed 8 October 2013).

[24] Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (July–September 2013): 365–404.

[25] Brandon Valeriano and Ryan Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51, no. 3 (May 2014): 347–60.

[26] The quote is from James Andrew Lewis, "Five Myths about Chinese Hackers," *Washington Post*, 22 March 2013. For skepticism of the threat of Chinese espionage to Western competitiveness and review of cybercrime loss literature, see Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Access, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (New York: Oxford University Press, 2015), chap. 2.

[27] Rid, "Cyber War Will Not Take Place," argues that cyber war is not war because it is not sufficiently violent. Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73, goes further to argue that cyber war fails to serve the traditional political functions of war.

significant, such as piracy, espionage, and "hacktivist" protest, even as the Internet is defense dominant for more harmful or complicated forms of attack. Serious cyber attacks against complicated infrastructure require considerable intelligence preparation, test and evaluation infrastructure, planning capacity, technical expertise, and complementary military or non-cyber intelligence assets.[28] If so, it would be a categorical error to mistake the frequency of irritant activity for a more general tendency toward offense dominance across the entire cyber domain.

Alternately, offense-defense theory itself might be incoherent or in need of repair, as some of its critics have argued. Offensive and defensive actions can be conflated at different levels of analysis (e.g., an armored counterattack can support the defense even as defensive entrenchment can support an advance). Technologies are also famously difficult to categorize as functionally offensive or defensive throughout the international system at any given time.[29] Offense-defense theorists rarely subscribe to a naïve technological determinism and usually include other variables in calculating the net assessment of forces, including geography, labor, organizational capacity, doctrine, and even diplomacy.[30] The offensive potency of blitzkrieg requires not only the tanks, radios, and aircraft, although these were critical, but also the doctrine of combined-arms warfare and the failure of the opponent to defend in depth. If "organizational force employment" considerations fundamentally shape the offense-defense balance, then it becomes more a matter of dyadic relationships rather than of a systemic effect of technology alone.[31] Cyberspace as an operational domain is highly sensitive to technological expertise and the ability to plan, coordinate, and execute complex operations, suggesting that factors other than technology should be at least as critical, and possibly even more important, in shaping the offense-defense balance in cyberspace as they are in traditional domains. These factors might not be the same in every engagement; it would be surprising if they were.[32]

---

[28] Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, April 2009, http://hdl.handle.net/10945/37162.

[29] See Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4, no. 4 (Summer 1995): 660–91; Glaser and Kaufmann, "What Is the Offense-Defense Balance?"; James W. Davis et al., "Taking Offense at Offense-Defense Theory," *International Security* 23, no. 3 (Winter 1998/9): 179–206; Keir Lieber, "Grasping the Technological Peace: The Offense-Defense Balance and International Security," *International Security* 25, no. 1 (Summer 2000): 71–104; Yoav Gortzak, Yoram Z. Haftel, and Kevin Sweeney, "Offense-Defense Theory: An Empirical Assessment," *The Journal of Conflict Resolution* 49, no. 1 (February 2005): 67–89.

[30] Glaser and Kaufmann, "What Is the Offense-Defense Balance?"

[31] Biddle, "Rebuilding the Foundations of Offense-Defense Theory."

[32] For an argument that offense-defense theory is not helpful for understanding cyberspace, see Keir Lieber, "The Offense-Defense Balance and Cyber Warfare," in *Cyber Analogies*, ed. Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School, 2014), 96–107, available at http://hdl.handle.net/10945/40037. For an opposite view, cf. Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (1 April 2013): 40–63, doi:10.1080/13523260.2013.771031.

Evaluating the general validity of offense-defense theory is beyond the scope of this article. Instead, we simply call into question the more contained consensus that offense has the advantage in cyberspace, given the manifest absence of high-intensity Internet aggression. Many of the assertions delineated above about disarming, deterring, and defending in cyberspace can be or have been criticized or modified. Still, our recitation represents a consensus in the cybersecurity discourse, and so confusion remains where we began. If all three strategies are ineffective against a determined attacker, then why is it that cyberspace has not already erupted into unremitting warfare? Something additional is needed to account for the apparent robustness and stability of the Internet. The troika of protective strategies assumes that no alternative exists that could either prove more effective or that would combine with deterrence and defense to form a more comprehensive, and potent, strategy set. In fact, there is a fourth option, one that has been overlooked conceptually if not operationally. Deception has been largely ignored by analytical studies thus far, much as deterrence received little intellectual attention prior to the nuclear age.

THE TECHNOLOGY OF DECEPTION

The Internet's potential for deception is a common yet unarticulated assumption in arguments about cyber offense dominance. The ubiquity of information technology provides attackers with opportunities to hide anywhere and abuse any data, potentially, so deception undermines disarmament. Anonymous hackers have many ways to disguise their identity, avoid detection, and mislead investigators, so deceptive attackers flout the credibility or effectiveness of deterrent threats. Infrastructural complexity enables attackers to exploit hidden vulnerabilities and gullible users, so deception facilitates the penetration of network defenses. Deception not only enables cyber attack, it is necessary: attackers who fail to be deceptive will find that the vulnerabilities on which they depend will readily be patched and access vectors will be closed.[33]

Deception of any kind manipulates information, showing what is false and hiding what is true, so it should not be surprising that technology designed to processes information also serves to facilitate deception. As information technology has grown more sophisticated, from the dawn of writing to the Internet, the opportunities for fraudulence and trickery have

[33] This inverts reasoning by Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security* 22, no. 4 (Spring 1998): 5–43, that offense dominance makes secrecy more likely, which in turn raises the potential for war ("Explanation H"). In cyberspace, secrecy comes first as enhanced potential for deception is required to change the offense-defense balance. However, as we argue, secrecy need not make conflict more likely if it also improves protection or makes attackers paranoid.

also grown more sophisticated. Gullible people and vulnerable machines are now linked together at an unprecedented scale. The risk of deception cannot be engineered away, moreover, because user trust and software abstraction are required in order for computer applications to be useful at all. Signals designed to certify the authenticity of communications simply become additional tools for deception.[34] Hackers send phishing e-mails to employees impersonating coworkers or give away infected thumb drives at trade shows in order to gain a foothold on protected networks.[35] Stuxnet combined a number of ruses, including antivirus detection and evasion, self-hiding propagation controls, and an innovative "man in the middle" attack that created bogus feedback for human operators in order to mask the alarms caused by malfunctioning centrifuges.[36] Similarly, the National Security Agency has employed various tools to "muddle the signals of the cell phones and laptop computers that insurgents used to coordinate their strikes" and "to deceive the enemy with false information, in some cases leading fighters into an ambush prepared by U.S. troops."[37] The Internet's capacity for deception is what facilitates its malicious use: no deception, no attacks.

The attacker can also be fooled, however, and the defender can also deceive. Offensive advantage in cyberspace depends critically on the potential for deception, but defenders also gain advantages from deception, provided opportunities are identified and exploited effectively. This ability to deceive—and to coordinate deception with complex strategies and operations—is analytically distinct from a systemic offense (or defense) dominance rooted in technology.

Strategic Manipulation of Information

Deception is a strategy designed to improve one's prospects in competition. It can deny a benefit to an opponent, as when camouflage, concealment, and decoys obstruct target discrimination. It can impose a positive cost, as when a sabotage or ambush creates casualties or a scam defrauds money. It may do both simultaneously, for example, by distracting the adversary from attacking vulnerable assets while covering a surprise attack in return.

---

[34] For example, websites certified as safe from malware by a well-known commercial authority end up being twice as likely to be untrustworthy as uncertified sites. See Benjamin Edelman, "Adverse Selection in Online 'Trust' Certifications and Search Results," *Electronic Commerce Research and Applications* 10, no. 1 (2011): 17–25.

[35] For a review of social engineering tradecraft for exploiting reason and emotion online, see RSA, *Social Engineering and Cyber Attacks: The Psychology of Deception*, White Paper (Hopkinton, MA: EMC Corporation, July 2011), http://www.rsa.com/products/consumer/whitepapers/11456_SOCENG_WP_0711.pdf.

[36] Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier*, White Paper (Mountain View, CA: Symantec, February 2011).

[37] These incidents refer to activity during the 2007 surge in Iraq, according to Ellen Nakashima, "U.S. Accelerating Cyberweapon Research," *Washington Post*, 18 March 2012.

Many deceptive ploys, especially in intelligence tradecraft, seek to create the illusion of cooperation so that the opponent does not even realize that it is being targeted until it is too late. Even if the target suspects a stratagem, it can still suffer costs in terms of the time and resources expended on operational security.

The two basic tactics of deception are dissimulation and simulation, or hiding what is there and showing what is not, respectively.[38] Sometimes the word "deception" is used only for active simulations that create bogus information to trick an opponent into taking the bait. We use the concept more broadly to cover also passive dissimulations, such as concealment and camouflage, that hide information opponents would want to know (and might act on if they were aware). Deception masks or adds information in order to influence indirectly the beliefs that affect an opponent's voluntary decisions to act.[39] This indirection is both a strength and a weakness for deception because the target acts willingly, but the desired action is not assured. Seduction promises influence with little overt conflict, but the deceiver has to be talented, careful, and lucky to translate a manipulative approach into a decision by the target to be manipulated in the desired way.

Not surprisingly, much of the literature on deception focuses on the psychological aspects of credibility. The deceiver acts to manipulate beliefs to produce false inferences.[40] Because deception provides competitive advantages, there are also advantages in being able to detect deceit. Primates have evolved sophisticated lie detection heuristics as well as hard-to-fake gestures like the facial expressions of love and shame.[41] A deceiver therefore must also work within the constraints of counter-deception efforts as well.[42] Intelligence scholar Richards J. Heuer Jr. points out that "deception seldom fails when it exploits a target's preconceptions. The target's tendency to assimilate discrepant information to existing mental sets generally negates the risks to deception posed by security leaks and uncontrolled channels of information."[43] Indeed, street conmen succeed in parting the gullible from their money even when hindsight reveals plenty of obvious clues—the wrong part

[38] Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies* 5, no. 1 (1982): 178–92; J. Bowyer Bell, "Toward a Theory of Deception," *International Journal of Intelligence and CounterIntelligence* 16, no. 2 (2003): 244–79.

[39] Here, "information" is used in the colloquial sense of suppressing or providing material signals. From an information theoretic standpoint, both dissimulation and simulation remove information, the former by suppressing signals and the latter by injecting noise. The net effect is that the target's decisions are governed by chance (or bias) rather than transmitted constraint. In either case, the deceiver creates degrees of freedom in the world that the target believes are constrained.

[40] Ettinger and Jehiel, "A Theory of Deception," 1.

[41] Paul Seabright, *The Company of Strangers: A Natural History of Economic Life*, rev. ed. (Princeton, NJ: Princeton University Press, 2010), 35–90.

[42] Paul E. Johnson et al., "Detecting Deception: Adversarial Problem Solving in a Low Base-Rate World," *Cognitive Science* 25, no. 3 (May 2001): 356.

[43] Richards J. Heuer Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981): 294. By the same token, schemes that seek to alter

of town, hurried actions, pressure tactics, conspiratorial bystanders, stereotypical frauds, etc. Deceiving entire organizations is perhaps more difficult because there are more individuals who might smell a rat, but deception can still work by exploiting organizational routines, corporate culture, and groupthink.

Deception in Practice

Virgil's *Aeneid* offers an example of deception so famous that it has become a byword for modern malware. Greek warriors intent on subduing Troy, but unable to scale its strong walls, instead resorted to the ruse of a hollow wooden tribute stuffed with Hellenic commandos. The Second World War featured several (in)famous plots in this spirit. The Allies concocted a bogus First US Army Group for Nazi eyes and ears, complete with phony radio traffic and inflatable tanks, all "commanded" by the flamboyant General George S. Patton. The ruse deceived Hitler and other German officials about the true location of the Allied invasion, leading to controversy and indecision in the Nazi high command and lessening resistance at the critical moment, on the beaches in Normandy. Allied diversions included other imaginative schemes like Operation Mincemeat, which planted false war plans on the corpse of a British soldier, and the Double Cross (XX) System, which fed disinformation through compromised Abwehr agent networks in Britain and Europe.[44] Tactical surprise, stealthy movement, and feints are commonplace, even essential, in modern-joint and combined-arms warfare, distracting the defender long enough for the main blow to be dealt from another axis (and potentially undermining peace negotiations).[45] Most of this activity, however, plays a distinctly secondary role in war and cannot be divorced from the material ability to inflict damage or to recover from deception gone awry. Deception is thus generally treated as a useful adjunct to the larger thrust of military operations.[46]

---

or implant, rather than reinforce, existing beliefs are much less likely to prove successful. Heuer provides a helpful summary table of cognitive biases and their implications for deception; see ibid. 315–16.

[44] Michael Howard, *Strategic Deception in the Second World War* (London: Pimlico, 1992); Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Scribner, 2004).

[45] Strategic surprise involves creating uncertainty about ends; by contrast, tactical surprise consists of keeping an enemy guessing about how means will be employed. Bahar Leventoğlu and Branislav L. Slantchev, "The Armed Peace: A Punctuated Equilibrium Theory of War," *American Journal of Political Science* 51, no. 4 (October 2007): 755–71, note that because "tactical surprise often is decisive for the particular engagement, and such an engagement could end the war," combatants capable of surprise attack have trouble credibly committing to a peace settlement.

[46] Deception (*maskirovka*) is an important aspect of Russian military doctrine and figures prominently in Russian writings on cyber strategy; see Dima Adamsky, "Russian Perspectives on Cyber (Information) Warfare" (paper presented at Rethinking Information and Cyber Warfare: Global Perspectives and Strategic Insights, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore, 3 March 2014).

The picture changes dramatically when shifting from military to intelligence operations. Indeed, most of the WWII-era British schemes mentioned above involved military intelligence operations targeting (pathologically credulous) Abwehr collection efforts. Deception is essential for secret intelligence, not just an optional adjunct. Secret agents use disguises and hidden signals to avoid detection by an enemy that can easily overpower the spy's meager self-defenses. If the covert sources or methods used to create a surreptitious information channel are compromised, then the target of collection can rapidly change its behavior or otherwise move secrets out of the spy's material reach. Alternatively, the target may elect to add another layer of deception by spying on the spy. The compromised agent can then be used as a conduit for disinformation.[47] The spy or her handlers, in turn, may suspect deception even when there is none and thus cast doubt on information the spy obtains. Paranoid suspicion alone degrades the effectiveness of intelligence collection. Disinformation operations can likewise be used against normal information channels for psychological purposes. The intelligence-counterintelligence contest is a funhouse of mirrors with endless possibilities for case officers and novelists alike.[48]

One legendary CIA counterintelligence operation during the Cold War targeted Soviet industrial espionage against the West. Through a "massive, well-organized campaign" known as "Line X," the Soviets recovered "thousands of pieces of Western equipment and many tens of thousands of unclassified, classified, and proprietary documents" that benefited "virtually every Soviet military research project."[49] Once alerted to the danger by a defector code-named "Farewell," the CIA arranged for altered versions of Western technology and scientific disinformation to make their way into Line X. According to one participant, "The program had great success, and it was never detected."[50] Thomas Reed reports that faulty control software installed on a Trans-Siberian oil pipeline caused "the most monumental non-nuclear explosion and fire ever seen from space."[51] This episode is frequently cited in the cybersecurity literature to illustrate the dangerous potential of attacks on material supply chains. What authors usually fail to emphasize, however, is that the Line X sabotage is also an example of successful defensive

[47] Sun Tzu distinguishes between "converted spies" (double enemy agents) and "doomed spies" (enemy agents subject to disinformation).

[48] Michael Herman, *Intelligence Power in Peace and War* (New York: Cambridge University Press, 1996), 176–180.

[49] Central Intelligence Agency, *Soviet Acquisition of Militarily Significant Western Technology: An Update*, September 1985, available at http://www.dtic.mil/dtic/tr/fulltext/u2/a160564.pdf.

[50] Gus W. Weiss, "The Farewell Dossier: Duping the Soviets," *Studies in Intelligence* 39, no. 5 (1996), available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm.

[51] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Random House, 2004), 269. Some dispute this account for want of corroborating evidence; see, for example, Rid, "Cyber War Will Not Take Place."

deception. Although Soviet agents were able to use offensive deception to penetrate Western industry, their actions also made them vulnerable to defensive deception conducted by CIA counterintelligence. Students of cyber strategy would do well to bear in mind that the Line X caper teaches lessons about both supply-chain insecurity and the disruptive potential of counterintelligence.

The Deception Revolution

Logistical friction bedevils military deception, and intelligence agents must take elaborate precautions to avoid compromise. Going to a café is easy; meeting a source who intends to betray his country at a café equipped with cameras and incognito policemen is far riskier. Intelligence collectors have been able to significantly reduce personal risk through arms-length technical collection since the dawn of the telegraph.[52] Targets attempted to protect their communications from eavesdroppers by shielding cables, guarding exchanges, encoding transmissions, and criminalizing unauthorized wiretaps, yet signal collectors in remote locations were hard to catch, and the benefits of spying were too great. Something additional was needed, not to prevent or inhibit an opponent from interdicting correspondence, but to make the effort futile. The resulting intelligence-counterintelligence contest gave rise to the modern profession of high-tech espionage.[53] In an intensively technological world there are more things to know, more ways to know them, and more ways to manipulate knowledge. The computer network exploitation we experience today is only the most recent manifestation of a long evolution of technological espionage.[54]

Rather than persuading Trojans to draw massive equine contraptions through unassailable city gates, cyber deception capitalizes on the fact that targets are already credulously immersed in a digitized infrastructure. Widespread faith in the Internet facilitates productive economic and administrative exchange, but by the same token, it is easy for a deceiver to exploit

[52] In Alexander Dumas's novel *The Count of Monte Cristo*, the protagonist wipes out an enemy's fortune by sending false information over the semaphore network. The Chappe semaphore preceded electrical telegraphy by five decades.

[53] See Daniel R Headrick, *The Invisible Weapon: Telecommunications and International Politics, 1851–1945* (New York: Oxford University Press, 1991); Peter J. Hugill, *Global Communications since 1844: Geopolitics and Technology* (Baltimore: Johns Hopkins University Press, 1999); David Paull Nickles, *Under the Wire: How the Telegraph Changed Diplomacy* (Cambridge, MA: Harvard University Press, 2003).

[54] Technology augmented age-old human intelligence (HUMINT) with new disciplines, like communication signals (SIGINT), photographic imagery (IMINT), underwater acoustics (ACINT), and assorted measures and signatures (MASINT). On the expanding scope of organizational control opportunities and challenges created by information technology in general, see James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, MA: Harvard University Press, 1986); JoAnne Yates, *Control through Communication: The Rise of System in American Management* (Baltimore: Johns Hopkins University Press, 1989).

this trust. Even the savviest users must assume that their software and hardware will perform as expected. It is simply not feasible to review every line of code and configuration setting, most of which are compiled or set prior to runtime by a multitude of vendors, developers, and network operators.[55] Those in the less technically savvy majority must utilize their e-mail and smart phones even less critically.

The targets for dissimulation or simulation now include not only the cognitive constructs of users but also the rules that designers have engineered into software code itself.[56] Software works by simplifying the world into models that can be readily computed and compactly encoded for transmission. For example, the original Internet protocols were designed to treat all machines the same and to accept connection requests from anyone on the network. The tight-knit community of computer scientists who invented the Internet had no reason to distrust one another, so they neglected to include security controls that would have increased the complexity of the protocols. That same openness later facilitated DDoS attacks that would flood servers with more connection requests than they could handle. The mismatch between the ideal software abstraction and the real variance in the world—in this case, an Internet with millions of potentially untrustworthy users—was later addressed by allowing servers to screen requests. DDoS programmers then looked for other mismatches in machine expectations, perpetuating the "arms race." Abstraction is the essence of software, yet deception exploits the variance between an abstraction or its implementation and the real state of the world.

As mentioned above, deception works indirectly by influencing the target's beliefs. The art of computer science notably depends on indirection to achieve impressive computational feats, but it thereby greatly expands the opportunities for deception. Indirection can be temporal through machine state and precompiled procedures, logical through programming abstractions and application interfaces, and spatial through distributed data and computing services. Software deception involves intervening in one of these existing layers of indirection in order to manipulate downstream processes that depend on it.

Evolution has equipped the human mind with sophisticated lie detection capacities that work by subconscious correlation of many different behavioral signals. Trust among primates is never absolute, of course, and

[55] For example, the Heartbleed bug, discovered in April 2014 in the OpenSSL protocol, was caused by a failure to check the length of a string in a ping request, an alarming flaw that was hiding for years in plain sight in openly available code developed and reviewed by security engineers.

[56] Some cognitive scientists argue that mental operations are literally extended beyond the skull via technological information-processing prosthetics. See Edwin Hutchins, "How a Cockpit Remembers Its Speeds," *Cognitive Science* 19, no. 3 (1995): 265–88; Andy Clark and David Chalmers, "The Extended Mind," *Analysis* 58, no. 1 (January 1998): 7–19; Andy Clark, "Curing Cognitive Hiccups: A Defense of the Extended Mind," *The Journal of Philosophy* 104, no. 4 (April 2007): 163–92.

suspicion may persist across interactions. However, in contrast to the subtle, high-context counter-deception heuristics that guide human face-to-face interaction, computers are more autistic. Deterministic algorithms either accept forged credentials completely or reject them completely, oblivious to social cues or shades of agreement. Cyber deception, once accepted, is often total. Even when software engineers write detailed error-checking routines or multifactor authentication schemes in an effort to increase context and error-correction channels, their deterministic code invariably overlooks use cases that can be exploited by an intelligent adversary. Well-written code can be caused to execute in unexpected circumstances (as when malware escalates privileges to the administrator level to install a rootkit) or to fail to execute when expected (as when antivirus software fails to detect and block a new malware signature). Once software engineers understand the mismatch between encoded simplifications and dangerous variation in the world (i.e., bugs), they strive to correct the discrepancies through debugging and patching, but these merely change rather than eliminate the simplification.[57] When machines mediate human interactions, they strip out much of the context primates rely on to establish gradations of trust. Low-context interaction is thought to account for some cyber bullying, offensive e-mails, and other bad Internet behavior.[58] The lack of context also makes it harder to detect social engineering scams that persuade users to part with passwords or provide access to machines. Deception is well-suited to the cyber domain, a global network of gullible minds and deterministic machines.

THE LIMITS OF OFFENSIVE DECEPTION

As useful and necessary as deception is for cyber attack, faith in the Internet is not misplaced for most users most of the time. On the contrary, critical financial, logistic, and public utility functions have moved online because, not in spite, of growing confidence in the reliability of network technology. In markets with highly asymmetric information, bad products should crowd out the good ones, yet the Internet has thus far not devolved into a pure "market for lemons."[59] Cyberspace should be a target-rich environment for digital

[57] Bugs emerge when an abstraction does not match reality, such as the Y2K bug caused when programmers used two digits to represent the year. Bugs become vulnerabilities when mismatches create exploitable opportunities for an adversary.

[58] Saul Levmore and Martha C. Nussbaum, eds., *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, MA: Harvard University Press, 2011).

[59] George A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics* 84, no. 3 (August 1970): 488–500. "Rippers" sell bogus credit card numbers and fraudulent hacking software to other criminals; see Cormac Herley and Dinei Florêncio, "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," in *Economics of Information Security and Privacy*, ed. Tyler W. Moore, Christos Ioannidis, and David J. Pym (New York: Springer, 2010), 33–53.

parasites, yet parasites are remarkably rare. The utility of the Internet has steadily improved.[60] Cyber attackers do not run rampant like raiders on the steppe because they are both limited by and subject to deception. Below, we consider how the reliance on fraud for offense actually incentivizes attackers to show restraint.

An oft-quoted passage from Sun Tzu reads, "All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[61] In reality, Sun Tzu's advice is easier given than followed. Carl von Clausewitz notes that surprise is both useful and difficult to achieve.[62] A potent military force takes time and effort to assemble. Large-scale preparations are difficult to conceal.[63] Smaller or simpler formations are easier to disguise, but they typically lack firepower or sufficient reserves, making them less potent on the battlefield. All forces require planning, manning, sustainment, and communications, but these activities are subject to mishaps and misperceptions. Clausewitz describes these problems as collectively subject to "friction" and the "fog of war." One tactical mistake or clue left behind could unravel an entire deception operation. Conspiracies have a way of being compromised, especially as the number of conspirators grows, but troops who are not in on the deceptive ruse might become just as confused as the enemy. Even if deception planning goes well, the target of deception may simply misunderstand the stratagem.

Large-scale military deception is logistically difficult to manage and depends on significant organizational integration, cooperative enemies, and luck. These conditions are rare. Surprise attacks of any significance—the Japanese raid on Pearl Harbor, the North Vietnamese Tet Offensive, Egypt's initiation of the Yom Kippur War, or al Qaeda's 9/11 attacks—are unusual events brought about as much by political conditions as by intelligence failures.[64] These attacks bring only temporary advantages for their perpetrators and more often than not invite fearsome retribution that eliminates the benefits of the original attack. These episodes, like the elaborate British deception conspiracies mentioned previously, are the exceptions that prove the rule that serious deception is difficult and rare. Countless schemes have

[60] Schneier, *Liars and Outliers*.

[61] Sun Tzu, "Laying Plans," in *The Art of War*, trans. Lionel Giles (1910; Project Gutenberg, 1994), http://www.gutenberg.org/ebooks/132.

[62] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), bk. 3, chap. 9.

[63] Because it is costly, mobilization can serve as a credible signal of resolve. See Branislav Slantchev, "Military Coercion in Interstate Crises," *American Political Science Review* 99, no. 4 (November 2005): 533–47.

[64] Richard Betts, *Surprise Attack* (Washington, DC: Brookings Institution Press, 1982).

no doubt been abandoned at the planning stage for want of adequate resources, command support, or feasibility, while other deception operations fail because they are impractical or poorly executed.[65] Commanders instead tend to emphasize attack and defense via mass and firepower. Tactical surprise and inventive maneuvers supporting larger military and naval efforts are prevalent, even essential, in modern warfare. These work best, however, in the service of hard military power—itself facilitated by deceptive cover, concealment, and maneuver—that is able to capitalize on the temporary windows surprise may create and to absorb setbacks produced by failed deception.

Cyber operations alone lack the insurance policy of hard military power, so their success depends on the success of deception. Martin Libicki points out that "there is no forced entry in cyberspace," meaning that all intrusions depend on a user or engineer leaving a logical door open.[66] Complexity is usually considered a disadvantage for cyber defense because it frustrates effective coordination, but complexity also complicates the tradecraft on which a targeted attack depends for the same reason. The most valuable targets tend to involve complex organizations, heterogeneous infrastructure, vast repositories of data, and critical tacit knowledge not exposed to digital recovery. Failure to control adequately for this complexity could result in mission failure when the malware "payload" does not perform as intended or nothing of value is exfiltrated from a target network. Failures to note the full range of defensive measures of the target network could result not just in mission failure, but also in retaliation.[67]

The risk of attacker compromise increases with the complexity of the target (which makes it more likely the attacker will leave forensic clues behind) and the seriousness of the attack (which makes it more likely the victim will mount a major investigation). Offensive deception thus reduces, but does not eliminate, the effectiveness of defense and deterrence. An attacker with a strong requirement for anonymity has strong incentives to show restraint.[68] Many cybersecurity measures seek to exploit the attacker's sensitivity to compromise by seeking to enhance authentication, intrusion detection, and

[65] There is a critical bias in the historiography of deception; successful ruses receive considerably more attention. For examples of schemes that were planned but not implemented, see S. Twigge and L. Scott, "Strategic Defence by Deception," *Intelligence and National Security* 16, no. 2 (2001): 152–57; Len Scott and Huw Dylan, "Cover for Thor: Divine Deception Planning for Cold War Missiles," *Journal of Strategic Studies* 33, no. 5 (2010): 759–75.

[66] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 31–36.

[67] The argument about cyber friction and target complexity is developed further in Lindsay, "Stuxnet and the Limits of Cyber Warfare."

[68] Nuclear terrorism is another threat that is supposedly premised by attribution problems. For a discussion of why political context helps the defender solve even technically difficult attribution, see Keir A. Lieber and Daryl G. Press, "Why States Won't Give Nuclear Weapons to Terrorists," *International Security* 38, no. 1 (Summer 2013): 80–104.

forensic attribution. Since the attacker must spend time reconnoitering a network to understand defensive threats and target opportunities (building up its situational awareness in a low-context environment), the defender also has more time to detect and observe the attacker. Unfortunately, standard security strategies by themselves can only be pursued so far. Computational remedies to computational vulnerabilities still must match logical abstraction with real-world variation, like any software solution. As we have seen, this is the very gap that cyber deception exploits, and more complex defensive measures simply provide more potential for deception. Deterrence in any case will not be effective against highly resolved attackers. Fortunately, there is another, more indirect, strategy to counter offensive deception.

FIGHTING DECEPTION WITH DECEPTION

Most of the literature on deception focuses on feints and ruses exercised by an aggressor to distract a victim.[69] Yet these techniques can also be implemented by defenders to foil an attack. Modern soldiers wear camouflage whether they are taking or holding territory. Insurgents likewise dress like civilians both to avoid targeting by security forces and to infiltrate them. As a protective strategy, deception differs from disarmament, deterrence, and defense in how it achieves protection. Whereas those three strategies seek to prevent, discourage, or block the attack, deception relies on the attacker getting through, at least to a degree. Both simulation and dissimulation rely on the dupe deciding to take the bait and walk voluntarily into the trap. Deception then uses an attacker's own capabilities and energy against it, by first inviting and then redirecting the attacker's self-interested action. Deception may even benefit the deceiver. In a meaningful sense, the deceived attacker can also be blamed for the punishment it receives.

Cyber attacks can be foiled not just by blocking intrusions, but by converting the penetration into something that confuses or harms the attacker. If it is easy for a covert attacker to gain access to an organization's data, it is also easy for a network protector to feed the attacker data that are useless, misleading, even harmful. The cyber attacker can become confused, even if the defender does not do anything deliberately, simply because of the inherent complexity and uncertainty involved in accessing and understanding remote computer network targets. The attacker cannot take for granted that

[69] Whaley, "Toward a General Theory of Deception"; Donald C. Daniel and Katherine L. Herbig, "Propositions on Military Deception," *Journal of Strategic Studies* 5, no. 1 (1982): 155–77; John Ferris, "The Intelligence-Deception Complex: An Anatomy," *Intelligence and National Security* 4, no. 4 (1989): 719–34; Roy Godson and James Wirtz, "Strategic Denial and Deception," *International Journal of Intelligence and CounterIntelligence* 13, no. 4 (2000): 424–37; Stefano Grazioli and Sirkka L. Jarvenpaa, "Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence," *International Journal of Electronic Commerce* 7, no. 4 (Summer 2003): 93–118.

all is as it seems. Indeed, in the practical world inhabited by security engineers, this reality has already begun to take hold. In this section, we clarify the utility of the protective strategy of deception and explore the strategy's applications to computer security.

Deception as a Distinct Protective Strategy

Disarmament, deterrence, defense (denial), and deception have always been available and appear intermingled throughout history, but shifting material conditions have necessitated rebalancing among strategies. If the information age makes defense and deterrence alone ineffective, as many experts believe, then reevaluating deception as a distinct strategic option would be appropriate. The heightened potential for deception in ubiquitous dual-use technology, whether used by the offense or the defense, bodes poorly for disarmament if risks cannot be reliably measured or proscribed. The implications for denial and deterrence are less straightforward because the defender can use deception to bolster each of these strategies.

Deception is logically different from denial even though they are often combined. Pure defense is the act of physically confronting attackers so that they cannot cause harm to the assets that are being defended. Deception, by contrast, conceals assets and pitfalls from the enemy. Castle walls protect a lord and his vassals by obstructing or canalizing invaders and by providing fighting platforms from which to repel an attack. Peasants seeking shelter in the castle can bury their wealth and hide their daughters in the forest to prevent plunder by either side. Those that stay and fight are practicing defense; those that flee after secreting assets engage in deception.

Armies once wore gaudy uniforms and employed tight, visible formations to improve coordination and esprit, thus optimizing for defense (or the attack). As the range, precision, and lethality of fires improved, however, armies began to emphasize deception—in the form of dispersion, cover, concealment, and mobility, along with a starkly different doctrine and training regimen—in order to keep the enemy guessing about their location. Navies likewise abandoned the line of battle in favor of dispersed formations and faster or stealthier vessels such as destroyers and submarines. Tactical deception so increased combat effectiveness that today we think of camouflage and dispersion as intrinsic to military organization and operations.[70] Yet deceptive measures are not themselves a defense, since cover and concealment alone do nothing to prevent an attacker from dominating the battlefield. Moreover, an active defense inevitably compromises deception as, for example, muzzle

[70] Deception does not always improve defense; it can also limit it. Artillery can be better concealed if shells are smaller and gun tubes shorter, but this takes away some of the lethality of firepower. Yet the general effect of deception as implemented in the modern system should be to improve overall military effectiveness.

flashes reveal the defender's location. Deception may be more or less effective when combined with the offense or defense, but deception as a strategy should not be confused with either of these actions.

In a similar fashion, deterrence differs logically from defense, even though the threat of a credible defense can serve to deter. Deterrence has always been a factor in world politics. Since antiquity, elites used the prospect of military mobilization to dissuade or compel their opponents. Yet because deterrence often failed, the ability to defend was critical in its own right. Nuclear weapons changed this calculus by making defense seem futile. Ballistic missiles capable of leveling cities could not be prevented or intercepted, thus promising unacceptable devastation. Policymakers were forced to consider strategies of pure deterrence in a world in which the prospect of annihilation made conquest meaningless but where threats of nuclear retaliation could still be useful tools of brinksmanship.[71] As Bernard Brodie famously observed, the object of strategy shifted from winning wars to avoiding them altogether.[72] Deterrence was bolstered by the inability to defend, and by the mutual prospect of unacceptable harm, even as deterrence skeptics sought counterforce options that would allow them to fight and win a nuclear war.

As nuclear weapons isolated, highlighted, and made the strategy of deterrence pivotal, so too cyberspace makes deception more salient as a regulating option in an increasingly wired and integrated world. Nuclear capabilities augmented the ability to deter even as they prevented effective defense. Similarly, cyberspace heightens the effectiveness of deception but with ambiguous implications for the other, more traditional, strategies. Deception is distinct from defense and deterrence as a strategy, but its effectiveness is expressed in combination with them.

Defense by Deception

Ubiquitous dependence on the Internet makes distinguishing malignant from benign activity difficult, thus foiling disarmament schemes even before participants can defect from them. For the same reason, however, it is difficult for the attacker to detect whether a virtual minefield has been entered. A cyber aggressor may be welcome, indeed encouraged, to penetrate a network. To encourage or even facilitate a cyber attacker to gain access to one's systems may make sense. As cyber spies vacuum up terabytes of data from a target's networks, what is to keep them from contracting a virus? As they open exfiltrated files, how can they be sure they have not installed malware that will subvert their own systems? Unable to distinguish between data that

[71] Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989).

[72] Bernard Brodie et al., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace, 1946).

are useful and data that are harmful, adversaries can be lulled into a false sense of security, even impunity.

Alternately, hackers may start to imagine that everything is a trap. They may worry whether their actions have tripped a silent alarm that will bring their activities to the attention of incident responders. As the adversary's intelligence analysts work their way through enormous haystacks, they must be alert to find both useful needles and dangerous ones. Deliberate defensive deception—real or feared—only exacerbates the intrinsic potential for attacker confusion. Deception adds to the ambitious attacker's already significant intelligence burden by: creating more use cases that attack code is required to handle; covering up heterogeneity so that all targets look similar; and hiding factors that can lead to failure against particular targets.[73]

Deterrence by Deception

Anonymity in cyberspace is by no means guaranteed. The defender's deceptive minefield can include broadcasting beacons that ensnare an attacker and follow it home, as well as silent intrusion-detection systems to provide attribution clues. A non-zero risk of identification means that the attacker cannot discount retaliation completely. Moreover, the adversary that would like to use deception to evade deterrence has no way to deter deception against itself. An adversary that wanted to complain about defensive deception would also have first to reveal its identity.

Even against an attacker that manages to remain anonymous, deception can still restore the threat of punishment. A duped intruder may punish itself by carrying a Trojan horse back with its plunder or getting lost amidst mountains of disinformation. Defensive Internet deception can provide a precision-targeted punishment. It is significant that only the transgressor is harmed by a decoy. A challenge of deception planning is to ensure that legitimate users do not become collateral damage of defensive-deception operations. Although this risk can never be eliminated completely in an intelligence-counterintelligence contest, it can be addressed by luring attackers into situations that authorized users would avoid. Some methods are discussed below. Even if the defensive deception is not completely successful, paranoia about the mere possibility of deception can reduce an attacker's confidence and encourage some degree of restraint.

[73] Attempts at deterrence or defense that do not employ deceptive dedifferentiation can inadvertently signal attackers as to the value of a target and therefore paradoxically encourage more attacks. Spreading defenses around may prove rational, as modeled by Robert Powell, "Defending against Terrorist Attacks with Limited Resources," *The American Political Science Review* 101, no. 3 (August 2007): 527–41.

Engineering Deception

Defensive deception is not just a theoretical possibility.[74] One of the first cybersecurity uses was by Clifford Stoll in 1986 after he detected attempts to break into the Lawrence Berkeley Laboratory network. Stoll created bogus systems and documents to assess the intruder's methods and targets. His bait included fake classified information to which digital alarms were attached. The hacker was eventually apprehended and found to be a West German citizen selling secrets to the KGB.[75] In the last decade, "honeypots" have become a basic tool of computer network defense. Lance Spitzner describes a honeypot as "an information system resource whose value lies in unauthorized or illicit use of that resource . . . If the enemy does not interact or use the honeypot, then it has little value." The honeypot works as a simulacrum of actual systems and files, databases, logs, etc. It is not only a decoy, but also an intrusion detection system: "By definition, your honeypot should not see any activity. Anything or anyone interacting with the honeypot is an anomaly." Spitzner also describes more complex "honeynet" systems of many honeypots or individual "honeytoken" files that an adversary might be encouraged to steal. The key is to design "a honeypot realistic enough for the attacker to interact with" that will vary depending on whether the intruder is a casual outsider or possibly a more knowledgeable insider.[76] Because one can expect intruders to start anticipating honeypots, engineers have even begun to experiment with "fake honeypots" in which legitimate machines try to look like an obvious honeypot in order to scare attackers away. The further possibility of "fake fake honeypots" begins to mirror the double agent games that are a fixture of spy novels.[77]

There are countless technical examples. A project sponsored by the Defense Advanced Research Projects Agency features a system of decoy documents and misbehavior sensors designed to protect distributed virtualized (cloud) data systems. Unauthorized access triggers a disinformation attack yielding bogus data nearly indistinguishable from live customer data. The authors argue that the system is useful for detection, confusion, and potential deterrence of adversaries.[78] Another project protects banking systems

[74] Jim Yuill, Dorothy E. Denning, and Fred Feer, "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques," *Journal of Information Warfare* 5, no. 3 (2006): 26–40; Kristin E. Heckman and Frank J. Stech, "Cyber-Counterdeception: How to Detect Denial & Deception (D&D)," in *Cyber Wargames*, ed. Sushil Jajodia (New York: Springer, 2015).

[75] Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (New York: Doubleday, 1989).

[76] Lance Spitzner, "Honeypots: Catching the Insider Threat," in *Proceedings of the 19th Annual Computer Security Applications Conference* (Washington, DC: IEEE Computer Society, 2003), 170–79.

[77] Neil C. Rowe, E. John Custy, and Binh T. Duong, "Defending Cyberspace with Fake Honeypots," *Journal of Computers* 2, no. 2 (2007): 25–36.

[78] Hugh Thompson et al., "Anomaly Detection At Multiple Scales (ADAMS)" (final report, sponsored by Defense Advanced Research Projects Agency, issued by US Army Aviation and Missile Command, 9

with dummy password-ID pairs. The only way for the attacker to distinguish between real and fake accounts is to try to extract money; the large number of decoys makes detection likely, allowing network monitors to observe the intruder's cash-out strategy.[79] Particular classes of hacker tools are also vulnerable to tailored counter-deception, such as a technique to flood key-logging malware with false data.[80] Other concepts include memory fragmentation and distribution schemes that make it difficult for an attacker to assemble a complete picture of the data with which the attacker is interacting.

The infrastructure that causes the greatest concern in the cyber war literature, industrial control systems, can also be protected by deception. One prototype generates deceptive network traffic coupled to simulated equipment to hijack the intruder's target selection process. Human subject testing with the prototype found that "counter attack vectors that lie in defensive deception are a viable approach to protecting electrical power infrastructures from computer network attacks."[81] Industrial complexity, "creates added difficulty in understanding the system, remaining undetected, and determining the steps necessary to cause significant damage . . . Deception can help turn complexity into an advantage for the defender."[82] Moreover, deceptive ruses need not work perfectly to be effective, and they can be combined for "deception in depth." In one real-time red-team versus blue-team cyber war game experiment, a honeypot system failed to deny red-team hackers access to the command and control mission system, but decoys and disinformation did succeed in preventing the adversary from obtaining sensitive data.[83]

Importantly, network defense and deception are not just conducted by mindless algorithms. Law enforcement agents and computer security experts are tactically active in the cyber defense ecosystem. Whereas an undercover agent like Joseph Pistone, alias Donnie Brasco, faces great personal risk

November 2011), http://www.dtic.mil/dtic/tr/fulltext/u2/a552461.pdf. In the same vein, another project floods an adversary with decoys and beacons; see Adam Wick, "Deceiving the Deceivers: Active Counterdeception for Software Protection" (research funded by US Department of Defense through US Small Business Innovation Research program, 2012), http://www.sbir.gov/sbirsearch/detail/393779.

[79] Cormac Herley and Dinei Florêncio, "Protecting Financial Institutions from Brute-Force Attacks" (paper presented at the 23rd International Information Security Conference, Milan, Italy, 2008).

[80] Stefano Ortolani and Bruno Crispo, "Noisykey: Tolerating Keyloggers Via Keystrokes Hiding" (presented at the USENIX Workshop on Hot Topics in Security, Bellevue, WA, 2012). Another technique uses decoy traffic through the Tor anonymizer to detect attempts at endpoint eavesdropping and HTTP session hijacking; see Sambuddho Chakravarty et al., "Detecting Traffic Snooping in Tor Using Decoys," *Recent Advances in Intrusion Detection, Lecture Notes in Computer Science* 6961 (Berlin and Heidelberg, Germany: Springer, 2011): 222–41.

[81] Julian L. Rrushi, "An Exploration of Defensive Deception in Industrial Communication Networks," *International Journal of Critical Infrastructure Protection* 4, no. 2 (August 2011): 66–75. The concept was inspired by Allied deception operations in WWII that used scripted conversations broadcast on German diplomatic radio channels.

[82] Miles A. McQueen and Wayne F. Boyer, "Deception Used for Cyber Defense of Control Systems" (paper presented at the Conference on Human System Interactions, Catania, Italy, 2009).

[83] Kristin E. Heckman et al., "Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment," *Computers & Security* 37 (September 2013): 72–77.

in infiltrating a criminal gang, Internet crime police can safely lurk in chat rooms and exploit the low context of Internet interactions to avoid criminal detection. If an online undercover agent is compromised, he just shuts down the compromised identity and starts a new one, with body parts and family members intact. Law enforcement stings, counterintelligence activities, and corporate network operators can all monitor and subvert attacker infrastructure.

Academic researchers also use deception as a methodology to study cybercrime, in order to discover better ways of combating it. Botnet control servers have been infiltrated by researchers who then use the criminals' own infrastructure to map the extent of compromise, their command and control methods, and their reaction to takedown.[84] A team of computer scientists from the University of California, San Diego poses as gray market customers, or sometimes as cyber criminals themselves, in order to study the economic structure of online illicit markets. Miscreant targets have responded by blocking the researchers' web crawlers, emitting bogus spam to confuse them, requiring voice contact from purchasers, etc., and the researchers have responded in turn with technical and human adaptations to overcome the criminals' countermeasures.[85] Over time, researchers have been able to identify major portions of the global spam and counterfeit pharmaceutical underground, particularly the financial infrastructure, and therefore aid law enforcement and official regulators with information leading to significant regulatory interventions and criminal prosecutions.

The everyday practice of cybersecurity has much in common with the classic give-and-take of intelligence-counterintelligence contests. Adaptations and counteradaptations occur on an ongoing basis in the shadows of the generally productive Internet. In global networked information systems, however, there are far more people involved in the deceptive game than ever before. The players now include engineers rather than just intelligence operatives and private and non-governmental sectors rather than just government officials. In other words, the rise of cyberspace has democratized deception. Attackers rely on deception to gain economic or political advantages, but they are also subject to deceptive exploitation by the very targets they attack.

[84] Chia Yuan Cho et al., "Insights from the Inside: A View of Botnet Management from Infiltration," in *Proceedings of the 3rd USENIX Conference on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More* (Berkeley, CA: USENIX Association, 2010), http://dl.acm.org/citation.cfm?id = 1855686.1855688.

[85] Kirill Levchenko et al., "Click Trajectories: End-to-End Analysis of the Spam Value Chain," in *Proceedings of the 2011 IEEE Symposium on Security and Privacy* (Washington, DC: IEEE Computer Society, 2011), 431–46; Chris Kanich et al., "No Plan Survives Contact: Experience with Cybercrime Measurement" (paper presented at the Workshop on Cyber Security Experimentation and Test, San Francisco, 2011).

DECEPTION AND THE OFFENSE-DEFENSE BALANCE

There is considerable potential for deception in cyberspace. Attackers deploy deception to undermine defense and deterrence in ways that seem novel, noteworthy, and threatening. Observers have thus inferred that offense has all the advantages. Indeed, for situations in which the attackers successfully maintain their stealth and the defenders fail to put up smoke screens or lay mine fields, offense is easy. However, defensive deception promises to delay significantly the intruder's exploitation of appropriated data, to burden opponents with false leads and sorting costs, and even to harm an attacker's technical infrastructure. If deception is easy, then both sides must learn to expect it. The spy-versus-spy arms race can go on indefinitely. Even if deception does not impose direct costs, paranoid counterintelligence efforts and operations security measures impose indirect burdens. Mutually assured deception is a boon for network protection. The result is to dull the power of a cyber offensive, even leading to unexpected stability as adversaries can no longer trust plundered data or be sure that an attack will perform as expected.

The net effect on the overall offense-defense balance remains unclear as data on deception are unsurprisingly difficult to collect or obtain. Perhaps cyberspace is still marginally offense dominant even if defenders use deception. We believe this is not the case. The cyber offense-defense balance is likely conditional on the complexity and severity of the attack and the resolve of the opponents. A high potential for deception, evenly distributed among the players, would yield offensive advantages against low-risk, low-reward targets while conferring defensive advantages for high-risk, high-reward targets. This logic echoes the classic stability-instability paradox and helps to account for the distribution of cyber conflict to date, with many relatively minor criminal and espionage attacks but few larger attacks that matter militarily or diplomatically.

Deception allows an attacker to intrude with low risk of detection or punishment, but only as long as it attacks objectives of relatively low value to the defender. The more effort that is required per attack, the less likely a target will be attacked.[86] As we have already noted, the majority of cyberspace nuisances indiscriminately attack homogenous resources. This occurs because the effort invested in an attack does not scale with the number of

[86] The majority of cyberspace nuisances indiscriminately attack homogenous resources, such as identical copies of software programs and standardized bank accounts, because the effort invested in an attack does not scale with the number of targets. It does not matter if untargeted scalable attacks fail against some or even most of the targets. Cormac Herley, "When Does Targeting Make Sense for an Attacker?" *IEEE Security & Privacy* 11, no. 2 (2013): 89–92. Nigerian spammers thus concoct ludicrous stories to filter out all but the most gullible victims, because sending bulk spam is cheap but responding to replies is much more costly; see Cormac Herley, "Why Do Nigerian Scammers Say They Are From Nigeria?" (paper presented at the Workshop on the Economics of Information Security, Berlin, 2012).

targets. For untargeted scalable attacks, failure against some or even most of the targets does not matter. As attacks become more ambitious, offensive costs increase in terms of planning, confusion, and risk.[87] Even without deliberate defensive deception, attackers must contend with sociotechnical complexity that risks failure and compromise. Furthermore, cyber criminals have only their computers to protect themselves from more intensive law enforcement or vigilante scrutiny. Most attackers will attempt to fly below the radar in order not to waste their resources, blow their cover, or invite retaliation. An enhanced potential for offensive deception is thus self-limiting.

Offensive advantages become much more tentative as risk exposure becomes more severe. High-reward targets—those systems and infrastructures on which an attack produces big financial, informational, or destructive outcomes—are more likely to be protected with defensive deception, including both intentional disinformation measures and the de facto complexity of internet-worked targets. These deceptive means are more likely to confuse, compromise, or injure the attacker due to the greater attention and higher deceptive posture of the defender and the innate complexity of the target. It is critical to understand that in such situations, deception is not acting alone. Instead, deception is reinforcing the effectiveness of the defense of high-reward targets and the deterrence of actors who might attack those targets. Where deception enhances defense, the ability to attack high-reward targets is less easy than is widely believed. Where deception enhances deterrence, those few with the ability to attack (currently limited to nation-states and high-end financial criminals) are likely to be dissuaded by fear of the consequences.

The existence of high-reward targets in cyberspace is a large part of what makes the cyber threat narrative compelling. Critical infrastructure and command and control systems are increasingly interconnected and, in principle, they are vulnerable to attack. The prevalence of attacks against low-reward targets by well-disguised attackers makes these high-reward targets appear to be all the more vulnerable. Yet appearances are misleading. The reality is that, although the technical possibility of attacks against high-reward targets can never be ruled out, the probability of a successful attack against a high-reward target is quite low. High-reward targets pose greater risks and costs to those that attack them. If the attacker cannot be sure that its anonymity is

[87] Advanced persistent threat (APT) espionage against particular firms in search of specific data requires greater per-target investment of time, effort, and skill. Thus, only firms with significant assets receive attention from APTs. APTs exploit homogeneity, such as widespread dependence on Microsoft and Adobe products, but they must still tailor operations to reconnoiter particular networks. Cyber weapons designed to disrupt complicated and inevitably heterogeneous industrial infrastructure will require even more per-target effort and expertise for preparatory reconnaissance and operational planning. Chinese APTs are very aggressive, but thus far they have shown restraint in not crossing from exploitation to disruptive attack, except against weaker opponents like ethnic minorities.

secure or the attacker has doubts that its malware will execute as intended (and without unwanted collateral damage or fratricide) or that its resources will not be wasted, then the benefits of attacking a target must be sharply discounted.

The asymmetric actors featured in cybersecurity discourse—rogue states, lone hackers, criminals, and terrorists—will tend to focus on the low-risk, low-reward bonanza and avoid deception-dominant high-risk, high-reward operations. Advanced industrial states will also partake in low-risk, low-reward espionage and harassment in cyberspace. Capable countries will, however, employ risky computer network attacks against lucrative targets only when they are willing and able to follow them up or backstop them with conventional military power. Because intelligence is costly and its exploitation is complicated, wealthier and larger states tend to have more sophisticated, robust intelligence capacities. Only capable actors, such as major powers, are likely to be able to master the complex tango of deception and counter-deception necessary to execute high-intensity operations. Powerful actors have an operational advantage in cyberspace. Even then, the frequency of complex and risky action should still be relatively low.

One type of cyber threat inflation, therefore, is the attempt to represent cyberspace as categorically offense dominant when there may in fact be relatively affordable defenses. Doomsday scenarios such as a "cyber Pearl Harbor" are useful in the pursuit of bureaucratic resources and autonomy. The potential for deception in cyberspace thus fosters a more politically motivated form of deception. Deception-prone environments increase the risk of threat inflation. A state that believes it is in an offense-dominant world may invest more in military and intelligence resources than is necessary or pursue capabilities of the wrong or suboptimal type. Yet if offense dominance does not apply to the most important targets—since they are protected by complexity and deception—then over-arming and sowing fear are wasteful and destabilizing. Resources that could be allocated elsewhere will instead be expended for unnecessary security measures. Such efforts might even interfere with economically productive aspects of the Internet. There is also the potential for tragedy if officials hastily resort to aggression in the mistaken belief that relations are fundamentally unstable. The disaster of 1914, when great powers rushed headlong into costly deadlock, reflected, in part, the impact of a mistaken "ideology of the offensive" applied inappropriately to what clearly turned out to be a defense-dominant reality.[88]

[88] Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1984).

STRATEGY IN A WORLD OF DECEPTION

This article argues for the salience of deception for both offense and defense. Indeed, deception has become essential for all types of operations on the airwaves or computer networks. Deception is essential for cyber attack because targets must be persuaded to leave the door open or distracted from closing it when there is no way kinetically to break it down. Yet its utility for cyber defense as well necessitates reconsideration of the superficially intuitive but overly deterministic claim that cyberspace is offense dominant. We further speculate that the offense-defense balance is not as unbalanced as usually believed and is in fact conditioned on attack severity, organizational competence, and actor resolve. This proposal will be difficult to test empirically as deception is, by nature, a self-hiding phenomenon. Evidence is likely to be more circumstantial in nature, such as reports of plans for active defense and deception protecting more high-value targets or of operators concerned about the validity of situational awareness when exploiting complex targets potentially guarded by deception. Incidents of low-cost, high-reward attacks, thus far largely absent, would potentially offer disconfirming evidence.

Strategic interaction in a deception-prone world is typically something other than war. Deception is an exploitative act that takes advantage of a competitor's preconceptions, which can be encoded in human minds or technological designs. It relies on ambiguity as opposed to the bright lines between war and peace. Deceptive operations in cyberspace are less aggressive than outright warfare but far from pacific. Deception matters most, politically, in increasing the options available for competitive and aggressive interactions other than war or for providing adjunct support to military operations. In this respect, computer network operations should mainly be understood as expanding the scope of intelligence and covert operations. As intelligence in general has become more critical for security operations and diplomacy, cyberspace is an important channel for information and influence. Intelligence has always been important in peace and war, yet now it involves a growing number of people both in and out of government service and organizations, as well as ever expanding budgets. The democratization of deception can account for both the historical continuity of cyber operations with intelligence and stratagem and their novelty in terms of ubiquity and complexity.

Locating the importance of cybersecurity in the inherent potential for deception opens up research possibilities yet to be explored. Submarine warfare, space control operations, human espionage, and special operations are also forms of interaction that fundamentally depend on deception. These areas might provide useful cases for comparison to alleviate the complaint that there is little empirical data available on cybersecurity. Notably, all the activities mentioned are useful in both peace and wartime. Even in war, deception is generally seen as an enabling adjunct, not as warfare itself.

Cyber warfare, and perhaps all forms of deception-dependent interactions, is best understood as low-intensity conflict behavior—whether in isolation in peacetime or as part of a military operation or, increasingly, in the ambiguous region between war and peace—rather than as a separate form of strategic warfare. At the same time, competition and conflict at the threshold of war can be complex and risky, reflecting both brinkmanship dynamics and the asymmetry and interdependence of parties tied together by mutual risk. This is clearly the case in the subsurface maritime domain: collisions between submarines led to negotiation of the Incidents at Sea Agreement to avoid inadvertent escalation between the United States and Soviet Union. Alternatively, cyber and other special or intelligence operations could provide a safety valve to help de-escalate crises and promote caution among adversaries that either fear being duped or discount the expected gains of aggression. The very secrecy of operations in space, cyberspace, or undersea is, however, what complicates strategic signaling immensely. Cyber warfare is not a "sui generis" phenomenon, but rather a member of a class of phenomena—intelligence and covert operations—that has received little scholarly attention, even as deception grows ever more complex and salient in strategic affairs.[89] Placing cyber operations in context with other forms of strategic and tactical deception can help to move the discussion beyond the debate over whether or not the cyber revolution is a disruptive innovation and begin to explore how cyber means actually work in conjunction with other strategic instruments.

There remain serious legal and policy considerations associated with this development that are beyond the scope of this article to address. In particular, the democratization of deception raises the problematic issue of cyber vigilantism, especially if private sector actors can use deception to counterattack ("hack back") threats. Some forms of defensive deception, for example that involve infecting an attacker's computer with a Trojan horse virus, might expose civilian defenders to liability under domestic laws such as the US Computer Fraud and Abuse Act. Uncontrolled deception could evolve from defensive deception to predation, somewhat akin to the great powers' experience with naval privateers, a practice that was eventually curtailed. Defensive deception also further exacerbates civil liberties concerns that were raised by recent revelations of pervasive Internet surveillance by the US government.[90] We do not mean to play down these practical challenges.

[89] Intelligence studies, a subfield of strategic studies, has tended to focus on historical operations or bureaucratic explanations for the behavior of intelligence agencies or political explanations for the use of intelligence by policymakers. There is comparatively little scholarship on the conditions under which intelligence influences policy outcomes, for better or worse, or the conditions that contribute to reliable intelligence advantage.

[90] The Edward Snowden leaks contain references to defensive-deception capabilities developed by the NSA, including bogus packet injection, redirects to phony servers, and other man-in-the-middle techniques to defend against cyber attacks on military networks. See Nicholas Weaver, "A Close Look at

Nevertheless, it is clear strategically that deception is now and will continue to become an attractive option for public and private actors in cyberspace.

ACKNOWLEDGMENTS

The authors would like to thank Ben Bahney, Kirill Levchenko, Austin Long, Heather Roff Perkins, Jacqueline Schneider, Frank Stech, and the anonymous reviewers for their helpful comments on previous drafts. This research was supported by the Department of Defense Minerva Initiative and Office of Naval Research Grant N00014-14-1-0071.

the NSA's Most Powerful Internet Attack Tool," *Wired*, 13 March 2014, http://www.wired.com/2014/03/quantum/.