A HOOVER INSTITUTION ESSAY

Strengths Become Vulnerabilities

HOW A DIGITAL WORLD DISADVANTAGES THE UNITED STATES IN ITS INTERNATIONAL RELATIONS

JACK GOLDSMITH AND STUART RUSSELL

Aegis Series Paper No. 1806

The Roman Empire's multi-continent system of roads effectuated and symbolized Roman military, economic, and cultural power for centuries. Those same roads were eventually used as a pathway for the Goths to attack and destroy the empire.[1] The Internet and related digital systems that the United States did so much to create have effectuated and symbolized US military, economic, and cultural power for decades. The question raised by this essay is whether these systems, like the Roman Empire's roads, will come to be seen as a platform that accelerated US decline.

We are not so foolish as to predict that this will happen.[2] But this essay does seek to shine light on the manifold and, in the aggregate, underappreciated structural challenges that digital systems increasingly present for the United States, especially in its relations with authoritarian adversaries. These problems arise most clearly in the face of the "soft" cyber operations that have been so prevalent and damaging in the United States in recent years: cyber espionage, including the digital theft of public- and private-sector secrets; information operations and propaganda, related to elections; doxing, which is the theft and publication of private information; and relatively low-level cyber disruptions such as denial-of-service and ransomware attacks.[3]

Our central claim is that the United States is disadvantaged in the face of these soft cyber operations due to constitutive and widely admired features of American society, including the nation's commitment to free speech, privacy, and the rule of law; its innovative technology firms; its relatively unregulated markets; and its deep digital sophistication. These strengths of American society create asymmetrical vulnerabilities in the digital age that foreign adversaries, especially in authoritarian

Jack Goldsmith is the Henry L. Shattuck Professor of Law, Harvard Law School.
Stuart Russell is a Visiting fellow at John F. Kennedy School's Belfer Center at Harvard University (on loan from the United Kingdom government). Russell works on the Kennedy School's Cyber Security Project. The views expressed in this paper are his own and do not represent the views of the government of the United Kingdom.

states, are increasingly exploiting. These asymmetrical vulnerabilities, in turn, might explain why the United States so often appears to be on the losing end of recent cyber operations and why US attempts to develop and implement policies to enhance defense, resiliency, response, or deterrence in the cyber realm have been ineffective. We do not claim that the disadvantages of digitalization for the United States in its international relations outweigh the advantages. But we do present some reasons for pessimism about the United States' predicament in the face of adversary cyber operations.

This essay proceeds in eight parts. Part I provides relevant background. Parts II through VII describe the six dimensions in which digitalization transforms a US strength into a vulnerability, especially by comparison with its impact on leading adversaries. The six dimensions discussed are global economic dominance, digital connectedness, a free and open society, government transparency, a commitment to the rule of law, and regulatory skepticism. After an analysis of these issues, part VIII briefly concludes.

I. Background

The digitalization of nearly every aspect of life, and the related rise of digital interconnectedness fostered by the Internet, has brought the US government and US citizens and firms enormous benefits on the global stage.

The United States subsidized the creation of the Internet. It led the global commercialization of the Internet that began in the 1990s. For over two decades, it controlled the Internet's naming and numbering system. And since the 1990s, its firms have dominated nearly every element of Internet and related communications technology: "Fifteen of the top 25 largest tech companies are from the United States, with eight in the top 10."[4] The so-called fearsome five—Google, Apple, Microsoft, Amazon, and Facebook—dominate their industry sectors and are the world's five most valuable companies and brands.[5] These multinational firms contribute enormously to the US economy and to US wealth. Through their dominance of the global Internet experience, their perceived embodiment of US culture and values, and their research and related funding, they have been an important element of US soft power.[6] Nations are resisting these elements of US power in various ways. But for now, the United States dominates.

US military and intelligence agencies have also reaped huge benefits from global digitalization. "We have more capacity than any other country, both offensively and

defensively," President Barack Obama claimed in September 2016 in reference to the United States' prowess in cyber operations.[7] The US military and intelligence budgets related to cyber operations dwarf those of other countries. Many news reports in recent years have described the United States' ability to penetrate foreign computer networks and to leverage the dominance of American Internet technology firms into robust intelligence-collection programs such as Section 702 of FISA.[8]

These are but some of the main large-scale international relations benefits that accrue to the United States from global digital networks. There are downsides as well. The many US economic, intelligence, military, and cultural assets embedded in digital form on computers and computer networks are potential targets for offensive operations from adversaries. These networks form very large attack surfaces that are generally hard to defend for many well-understood reasons:[9]

- The networks inside the United States are largely in private-sector hands or at least are connected mainly through private-sector communication channels.

- Computers and computer networks (software and hardware) invariably contain vulnerabilities that can be exploited to gain entry.

- The number of threatening offensive actors has exploded due to the fact that any computer connected to the Internet is potentially accessible to anyone on the Internet.

- Cyber-weapons—and especially the weapons and tools needed to carry out the soft operations that are the focus of this essay—are inexpensive to develop and deploy and thus are widely available.

- The Internet practically eliminates distance as a barrier, which means that offensive actors can hit the United States from practically anywhere.

- The Internet's architecture makes anonymity and spoofing (fake emails or web pages disguised to appear genuine) easy, which further facilitates unauthorized entry.

- Digitalization enhances the impact of insider threats.

- Compared to nondigital systems, digital systems permit enormous scaling by adversary actors of exploitation, copying, circulation, and attack.

In sum, the digital revolution brings the United States scores of benefits, but it also empowers many more adversary actors, from weak and strong countries alike, to harm the United States from a distance. Despite much work and significant improvements in recent years, especially in attribution, these harms have proved hard to stop or deter.

II. Private-Sector Global Economic Dominance

The first strength that has proved to be an asymmetrical vulnerability is the United States' global economic dominance. At present, private firms in the United States (and in Western nations generally) possess most of the intellectual property, trade secrets, and other proprietary commercial information (including negotiating positions, news of impending deals, and the like) that are worth stealing from the private sector.

In the last two decades, these important business secrets have increasingly become embedded in digital form. With the rise of the Internet and ever-more-powerful digital storage and copying capacities, orders of magnitude more cyber thieves—both insiders and thieves from around the globe—have potential access to these secrets and have been stealing them regularly. The result is that hundreds of billions of dollars of US business secrets have allegedly been stolen in the last decade in what former NSA director Keith Alexander has called the "greatest transfer of wealth in history."[10]

China-based hackers closely related to China's government have been the most notorious but certainly not the exclusive culprits in this transfer. (It has been widely reported, for example, that France, among other countries, engages in widespread economic espionage to benefit French businesses.[11]) During the last decade, China's firms possessed relatively few commercial secrets worth stealing and deploying to US commercial advantage. This situation is changing. China's firms are becoming technologically more innovative on many dimensions, and in some areas—such as mobile payment systems—they have a technological edge over US firms.[12] China thus has an increasing number of business secrets that may be useful to foreign competitors. But for now and the foreseeable future, an asymmetrical consequence of US economic strength is that US firms have many more business secrets that can and will be stolen via cyber means. This does not mean that US commercial prowess is, per se, a weakness. It just means that one consequence of digitalization is that US firms have an asymmetrical vulnerability to the theft of business secrets compared to Chinese firms.[13]

The asymmetry created by US commercial strength goes deeper than the distribution of valuable business secrets. The United States has long had a policy of not stealing

"the trade secrets of foreign companies on behalf of [or giving the intelligence it collects to] US companies to enhance their international competitiveness or increase their bottom line."[14] Despite its losses of the last decade, it has continued to adhere to this policy. The policy is not a result of the United States decoupling national security concerns from economic concerns. In a variety of contexts—export controls, CFIUS review of foreign investments, the Defense Department's close relationship with military contractors, and many more—the US government is sensitive to the national security implications of the domestic economy. Rather, the policy appears to result from a combination of two factors.

First, China and other less developed nations have relatively few commercial secrets for the US government to steal. This is changing, as noted above, but for now remains true. Second, and unlikely to change anytime soon, the United States does not have many state-owned industries and does not have a principled basis on which to distribute the stolen information to US firms, almost all of which are in the private sector. Alibaba and Tencent may have technological secrets in, for example, mobile payments that would be of benefit to US firms. But if the US government stole those secrets, who would it give them to? Apple? Google? Amazon? Such wealth transfers, which would have to be secret, are out of bounds for the United States, a democratic free-market society with few state-owned industries. By contrast, the decision to steal and distribute is much easier, and indeed natural, for countries like China with state-owned or state-connected businesses that the government wants to aid, and perhaps even for democracies like France that have large and important ownership stakes in globally competitive firms like Airbus, Air France-KLM, CNP Assurances, and Renault.

These are some of the reasons why most forms of commercial cyber theft—unlike, say, state-on-state espionage—are not symmetrical. China steals from US firms to help local industries, but the United States does not reciprocate because reciprocity via cyber is not presently an option in the US repertoire. That means that one important response tool to digital theft—reciprocal retaliation—is unavailable, leaving only tools that many believe are insufficient (such as economic sanctions or indictments) or tools that are unusable (such as military force).[15]

This example shows how a change in technological paradigms can have asymmetrical distributional consequences. Of course, the United States reaps countervailing benefits from digitalization vis-à-vis China in terms of, for example, espionage against government entities or the enormous financial gains that US Internet technology firms reap from access to the Chinese market. And of course there are downsides to imitative

development that China is trying to rectify. We neither deny these countervailing considerations nor seek here to assess how they cash out on balance. Our only point is that along the dimension of commercial progress via theft, the digital age empowers China and weakens the United States in relative terms.

The United States for years cajoled China to stop commercial cyber theft with threats that seemed remarkably weak given the stakes. In September 2015, China and the United States agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[16] This agreement extends only to government-sponsored theft or "knowing support" for such theft, not theft by the commercial sector without government support.

The consequences of the agreement are practically impossible to assess based on current public information. Many reports have indicated that China's government-connected commercial theft from the United States has diminished, though not ceased,[17] and some give credit to the agreement and related US diplomatic engagement.[18] Others offer less-consoling reasons. First, China's government hackers now hide their tracks better when they support commercial theft.[19] Second, Xi's "anti-corruption campaign" may be "cracking down on the illegitimate use of state resources."[20] Third, China may be slowing down its commercial theft abroad because its own economic development makes such theft less important.

While the situation is hard to assess with confidence, the digital commercial theft of US business secrets from China clearly has not ceased, and there is little reason to think it will in situations where such theft serves important government interests in China. As a US Trade Representative study concluded in March 2018, "Beijing's cyber espionage against US companies persists and continues to evolve," and "the evidence indicates that cyber intrusions into US commercial networks in line with Chinese industrial policy goals continue."[21]

III. Digital Connectedness

A related element of US economic and technological strength is the deep penetration of digital networks into everyday life. The United States is among the most digitally connected societies in the world. This deep digital connectedness, which can also be seen as deep digital dependence, roughly correlates with vulnerability to offensive cyber operations. It means that the United States typically has many more targets

for adversary offensive cyber operations, and that it is unusually vulnerable to such operations, compared to most of its adversaries. Given the relative ease of soft cyber operations, and the astounding number of potential attackers from abroad and targets inside the United States, the result is a serious disadvantage for the United States, especially vis-à-vis digitally unsophisticated adversaries.[22]

To see the point most starkly, consider the polar positions of the United States and North Korea. The United States has redoubtable offensive cyber capacities, and North Korea as a society is digitally underdeveloped. This means that the options for cyber operations against North Korea are relatively limited, irrespective of the United States' operational and technical sophistication. North Korea is not cut off from computers and the Internet altogether. But cyber tools do not work that well against North Korea because there is relatively little digital information to steal or digital infrastructure to alter or degrade.

By contrast, even though North Korea is digitally undeveloped, it does not take much skill or many resources to cause serious harm to the digitally dependent United States. The Sony hack attributed to North Korea caused up to $35 million in damage to Sony, plus whatever deterrent effect (on the development of anti-Kim films, for example) it achieved.[23] The *New York Times* reported last year that North Korean hackers, relying in part on NSA hacking tools that had seeped into the public realm, have stolen hundreds of millions of dollars in the past few years (globally) through ransomware.[24] North Korea was reportedly one spelling error away from stealing $1 billion from the New York Federal Reserve in 2016.[25] A more recent report concluded that North Korea's cyber army "is quietly morphing into one of the world's most sophisticated and dangerous hacking machines" and that since 2017 its "fingerprints have appeared in an increasing number of cyberattacks, [and] the skill level of its hackers has rapidly improved and their targets have become more worrisome."[26]

A former deputy director of the National Security Agency, Chris Inglis, explained North Korea's cyber power as follows:

> Cyber is a tailor-made instrument of power for [North Korea]. There's a low cost of entry, it's largely asymmetrical, there's some degree of anonymity and stealth in its use. It can hold large swaths of nation state infrastructure and private-sector infrastructure at risk. It's a source of income. You could argue that they have one of the most successful cyberprograms on the planet, not because it's technically sophisticated, but because it has achieved all of their aims at very low cost.[27]

The point has implications beyond cyber relations, since North Korea can leverage its cyber power in other domains. As the *Times* reported: "Mr. Kim, fearful that his nuclear program is becoming too large and obvious a target, is focusing instead on how to shut down the United States without ever lighting off a missile."[28] It then quoted Robert P. Silvers, the assistant secretary for cyber policy at the Department of Homeland Security during the Obama administration: "Everyone is focused on mushroom clouds," Mr. Silvers said, "but there is far more potential for another kind of disastrous escalation."

Silvers's point about escalation has much broader and, for the United States, more serious implications. Indeed, it appears that the fear of losing in escalation due to asymmetrical digital dependence is one of the main reasons why the US government has hesitated to retaliate in recent years in the face of increasingly damaging cyber operations from abroad. The fear is that any response by the United States to a cyber intrusion will result in a counterresponse that, since the United States tends to be more digitally dependent and vulnerable than its adversaries, will leave the United States in a worse place. This is reportedly a primary reason why President Obama hesitated before the 2016 election to respond to the Russian information operation.[29]

It is also the main reason why the United States did not respond forcefully to Iranian denial-of-service attacks on US banks in 2012. As former director of national intelligence James Clapper explained, the United States feared it would lose in escalation. "We'd all built up quite a head of steam, [thinking] 'By God, we're not going to let the Iranians get away with this! We're going to do something!'" Clapper said, describing the initial conclusions of a 2012 National Security Council meeting. "We had teed up a bunch of options for cyberattack against the very same players who had participated in these denial of service attacks [against the banks]," he said, adding that "the initial instinct was: Let's attack back."[30] But the NSC aborted the planned retaliation after then secretary of the Treasury Tim Geithner argued that US banks could not withstand the counterretaliation, Clapper explained. Of course, other competing demands, such as not wanting to disrupt the then pending Iran nuclear deal, might also have been in play.[31] But senior US leaders have emphasized that asymmetrical digital dependence and the related fear of losing in escalation is a primary hurdle to US responses to harmful cyber operations.[32]

One might wonder why the United States appears (or is assumed) to have escalation dominance in other realms (for example, air power and nuclear weapons) but not in cyber. And one might be especially puzzled since nothing in US military doctrine

precludes the United States from using its kinetic military weapons or from aggressively wielding its estimable economic might in response to adversary cyber operations.[33] The answers to these questions are complex and generally beyond the scope of this essay, but they likely include some combination of four factors.

First, as explained in more detail below, the soft cyber operations at issue here do not violate international law, especially not in a way that permits the United States to respond with kinetic force. Adversaries can do a great deal of damage with soft cyber operations, both initially and in escalation, below a threshold that would trigger a dominant US kinetic response. The United States might have escalation dominance above that threshold but not below it. Second, relatively inexpensive and easy-to-deploy weapons for soft cyber operations might allow a relatively weak adversary to escalate for more rounds and with greater success against a digitally vulnerable United States than is the case with more expensive kinetic weapons.

Third, since (as noted above) the United States' vulnerability to escalatory retaliatory cyber operations is not limited to retaliation for cyber operations, it might be that the United States has less certain escalation dominance in kinetic realms than is widely believed, but the point has not yet been tested or appreciated. Fourth, various forms of economic entanglement or interdependence might be working alongside escalation fears to preclude retaliation.[34] The Obama administration for a long time worried about imposing severe sanctions in response to Chinese commercial theft less for fear of Chinese cyber retaliation than for fear of Chinese retaliation against US firms doing business in China.

IV. A Free and Open Society

The benefits of living in a free, open democratic nation are too obvious to list. The conventional wisdom two decades ago was that the Internet would be a powerful force in favor of democracies in the struggle to open up totalitarian states and make them free.[35] This conventional wisdom is being flipped on its head because of another asymmetry between the United States and its authoritarian adversaries: a closed, authoritarian society like Russia does not face the same threat from adversary digital information operations as an open, free society like the United States.

Russia constricts and regulates the sources of news information and does not depend on a genuine democratic election process that can be disrupted by manipulating public information.[36] The United States, by contrast, has democratic elections, extravagant freedom of speech, and a notoriously free and unregulated news media. It is much

easier for an adversary to achieve desired effects through social media, to engage in successful doxing operations, to promulgate fake news, or to engage in online propaganda when there are multiple news and information outlets that are not under the control of the government. "We do have some special challenges" in confronting operations like the ones that Russia pulled off in 2016, Obama acknowledged, because "we have a more open society and engage in less control and censorship over what happens over the Internet, which is also part of what makes us special."[37] Digital networks in an open society not only make it easier to spread false or disruptive information; they also make it harder to counter the false or disruptive information with truthful, coherent information.

The point here is not that information operations or propaganda efforts do not work in authoritarian states. The history of the Cold War shows otherwise. So too does Vladimir Putin's claim that Hillary Clinton's State Department was the organizational force—perhaps assisted by digital tools—behind the anti-Putin protests in connection with Russian legislative elections in 2011.[38] Nor are all authoritarian states alike in their ability to deflect information operations. China has a robust domestic Internet that is in some dimensions lightly regulated, and it is likely more susceptible to foreign information and propaganda efforts than the Internet in Russia, where citizens engage in less robust Internet activities, especially on mobile devices.

But the United States is especially susceptible to all stripes of adversary information operations. Unlike in Russia and China, citizens in the United States elect leaders through autonomous votes that the government cannot lawfully control. Influencing citizen beliefs and preferences can thus have a big impact on leadership. Also, US citizens' beliefs and preferences are unusually susceptible to outside influence. The United States (like China, but unlike Russia) has a robust Internet culture where news promulgation is dominated by the Internet and especially social media. Most significantly, and in sharp contrast to China and Russia, the US government barely regulates digital content and is constitutionally restricted from regulating digital content related to political speech.

Consider doxing, the practice of publishing true and damaging (and often stolen) information about someone or some institution. A central element of the Russian operation in 2016 was the phishing attacks that stole information from the Democratic National Committee and then released it to the public.[39] An equally important part of this operation was releasing the stolen information in daily increments that ensured continuous, extended, and amplified coverage through the US media. Just as the 9/11 attacks used airplanes, a valued commercial instrument,

as a weapon, Russia weaponized the US media. The US media, in turn, churned the information released by Russia to Hillary Clinton's detriment in ways that the US government could not even think about trying to control. And once it became clear that the operation was sponsored by Russia, the politically fragmented US media churned that information, too, in ways that the government could not control. The ongoing investigation of the Russian operation has proved to be politically divisive, has called into question the legitimacy of US electoral integrity, and has further fragmented American society—once again, in ways the government could not attempt to manage.

Now consider, by contrast, Putin's allegation that the Panama Papers, which revealed corruption by Putin and other Russian oligarchs, was a US-led doxing operation.[40] Putin's malfeasance, as revealed in the Panama Papers, was far more damning than anything that was revealed by the DNC hack. Surely the release of the Panama Papers harmed Putin's reputation to some extent, at home and abroad, at least before some audiences. But Putin himself controlled coverage of the Panama Papers inside Russia, and he continues to control any "electoral" consequences of the fallout from the Panama Papers.[41] There is no equivalent in Russia to the Senate and House intelligence committees and the special counsel's investigation of the Russian operation. And as Putin's recent reelection confirms, there is little evidence that the release of the Panama Papers has caused political disruption in Russia.

V. Government Transparency

The US government is more transparent about its cyber operations, both on offense and defense, both its successes and failures, than any nation in the world.[42] It is certainly more transparent in these respects than any other superpower, and it is significantly more transparent than its authoritarian adversaries. Transparency in this context can have benefits, including (in some instances) accountability, but it also has downsides. The type of transparency that concerns us for present purposes is transparency about cyber losses.

We can assume that other nations suffer cyber losses akin to the Office of Personnel Management hack, the hack of the F-35 Joint Strike Fighter plans, the DNC hack, and the like. But the United States is the world's leader in *acknowledging* these losses to the public. It likely does so for several reasons. In the United States' unusually open media environment, and with its unusually robust and open oversight (again, compared to adversary nations), many of these losses would leak to the public in any event, and so the US government sometimes discloses them in anticipation. The governments of China and Russia do not face similar pressures. When (as in the OPM hack) the

losses impact the privacy and possibly the security of US citizens, the democratically accountable US government must acknowledge those losses to protect its citizens, but authoritarian governments need not do so.

In addition to the cyber losses that the United States discloses voluntarily, the US government is also the world's leader in involuntary disclosure of cyber losses—that is, leaks or insider theft. No government in the world suffers nearly the number or scale of public leaks of sensitive secret information related to cyber operations as the US government. In the digital age, leaks by insiders are much more consequential because information is so much easier to copy, steal, and disseminate than in the predigital era. A US leaker can now walk out of a government building with a mainframe in her back pocket.[43] (Compare Chelsea Manning's and Edward Snowden's insider leaks, in which massive amounts of information were exfiltrated quickly on small memory devices, to Daniel Ellsberg's months-long effort to exfiltrate and photocopy the Pentagon Papers.)

Part of the reason the United States suffers more public leaks in this area is that it has an enormous intelligence bureaucracy and thus has more secrets that, because of its size, are harder to keep.[44] Two other reasons explain the leaks. First, the First Amendment and the constitutional culture that has grown up around it mean that publishers in the United States suffer relatively few, if any, penalties for publishing classified information.[45] Second, the United States treats leakers (and spies more generally) much less harshly than other nations, and especially its authoritarian adversaries. The Obama administration pursued more leak investigations than any prior presidency, but very few people went to jail, and the vast majority of reported leaks result in no investigation or no prosecution. The United States certainly doesn't poison spies, for example, as the Russians allegedly did to Sergei Skripal in the United Kingdom even after his arrest, conviction, and transfer to Great Britain in exchange for Russian spies.[46] These latter two factors mean that the costs for the individual of leaking sensitive information are relatively low in the United States compared to authoritarian states.

The asymmetry in US government transparency about cyber losses harms the United States in two very different ways. First, and obviously, to the extent that the United States is asymmetrically vulnerable to leaks and related insider threats, it suffers asymmetrical intelligence losses. Second, the United States' asymmetrical disclosure of cyber losses—involuntary as well as voluntary—emboldens adversaries and weakens deterrence. The second point requires some explanation.

When losses from various forms of cyber operations appear on the front page of the newspaper, adversaries are made aware in a concrete and credible way about US vulnerabilities. Citizens expect the government to do something about the losses, and the government feels pressure to identify the culprit and act against it in some way. And so, after a major acknowledged cyber operation in the United States, the US government goes through a process of public attribution—for example, pointing to North Korea for the Sony hack, China for the 2015 OPM hack, Russia for the 2016 DNC hack and the 2017 NotPetya attack, and Iran for various cyber intrusions.

But having raised the issue of intrusion and attribution, the US government response becomes salient and visible. And for various reasons, the US public responses to these and other harmful cyber operations has been nonexistent or tepid. The main forms of public response have been indictments and relatively weak sanctions. In no case have these public responses been proportionate to the acknowledged losses the United States suffers. The publication of the many losses, followed by the invariably weak or nonexistent public response, demonstrates credibly that US defenses are poor and that the US government is either unable or unwilling to retaliate even in the face of massive cyber losses. This combination of events thus emboldens adversaries and weakens deterrence. Even if the United States is robustly engaging in retaliatory covert or clandestine responses, those responses cannot contribute to deterrence against the many third parties who are watching, and indeed in context detracts from it.

We can summarize the main point of this section as follows. Unless a nation is able to effectively redress a cyber intrusion, it can be harmful or self-defeating to publicize it, since public knowledge of loss and the failure to respond effectively invite more attacks.[47] The United States finds itself in the unfortunate position of having an asymmetrical lack of control over the publication of losses *and* not being able to effectively respond to those losses. Every digitally connected nation has trouble defending against and responding to cyber intrusions, but the United States is the world's leader in openly advertising its weakness in both defense and response, and it suffers accordingly.

VI. Rule of Law

The United States has the most legalistic intelligence and military bureaucracy in the world, and these legalisms extend to the cyber realm. This commitment to law, and to legal constraint, is a hallmark of the legitimacy of intelligence and military action in a democratic society. In that sense, it is a source of strength.[48] But it is also a source of

relative weakness. US adversaries—for example, China, Russia, Iran, and North Korea—are much less legalistic and much less constrained by law, domestic or international. The result in the cyber realm is that the United States is relatively hampered, domestically and internationally, in ways that benefit its adversaries.

First, the United States restrains itself from addressing information threats at home. Because of privacy and related values grounded in the First and Fourth Amendments and related statutes, the government has limited access to largely privately controlled networks inside the United States through which attacks from abroad travel. The United States is legally constrained from taking steps that might improve cybersecurity (broadly conceived) from both domestic and foreign threats. For example, China has comprehensive potential access to domestic communications, demands access to encrypted communications and to source code, has formal rules against anonymity, and can instantly order shutdowns based on content. The US government can do none of these things.

Second, the US government restrains itself from taking advantage of foreign adversaries' weaknesses, or from responding to threats from adversaries abroad, because of both domestic and international law concerns. Not only does the US government have a policy of not stealing foreign commercial secrets for the benefit of US firms; it also makes it a crime for US firms to steal such information from foreign rivals' computer systems.[49] Also, US law prohibits the CIA from engaging in a covert operation abroad "which is intended to influence United States political processes, public opinion, policies, or media."[50] The meaning of "intended . . . influence" in this prohibition is uncertain, but the prohibition surely limits US information operations abroad in ways that authoritarian adversaries are not limited.

The United States also takes international law constraints on cyber operations more seriously than its authoritarian rivals do. First, international law does not permit the United States to respond with kinetic force to the damaging soft operations that are this essay's focus because such operations do not rise to "uses of force" or "armed attacks" under the Charter of the United Nations.[51] Second, lawyers constrain US cyber operations due to concerns about violations of the sovereignty of "neutral" countries. According to Clapper, when the United States discussed cyber tools to use against North Korea in response to the Sony hack, the plan required going "through some other country's infrastructure"—perhaps China's.[52] "The lawyers went nuts, so we didn't do anything on the cyber front," Clapper says. "We ended up sanctioning a bunch of North Korean generals." Compliance with international law rules about proportionality and avoiding harm to civilian non-combatants have also hampered US cyber warriors. The US

government has "an inclination to be very precise, very limited, very surgical, legalistic," Clapper says. "You cannot be assured that the adversary is going to be similarly precise and surgical and legalistic."

To the extent that Clapper is right—and he is in a position to know—the United States is more constrained in using its cyber tools than its adversaries are.[53] Considered narrowly, this asymmetry weakens the affirmative use of cyber tools overtly and hampers deterrence by contributing to the US hesitation to respond to adversary cyber operations for fear of losing in escalation.[54]

VII. Regulatory Skepticism

The final asymmetry concerns the United States' relatively hands-off regulatory approach to digital networks, as compared with both other Western countries (for example, the nations of the European Union) and authoritarian countries. The relative paucity of regulation has been the hallmark of American Internet policy for two decades, and it is thought to be a central reason (but certainly not the only one) for US firms' extraordinary record of innovation and the extraordinary economic and other gains that flowed from these innovations.

The commitment to the relatively light regulation of digital firms and the Internet more broadly is akin to the constitutional hurdles to more government involvement in the domestic networks, but the limitation here is cultural or ideological, not legal. That does not mean that it is easy to change. On top of the cultural aversion to regulation, US Internet technology firms and their supporters claim they would lose their innovation edge and significant wealth with anything more than relatively light regulation from Washington.

To date, these firms' antiregulatory posture, and the lobbying and rhetorical muscle behind it, has been successful. This might be changing to some degree in light of Washington's recent interest in responding to some of the perceived excesses of social media and of data-collection practices by major US firms. But many are skeptical that this interest will materialize into meaningful regulation of US firms, and in any event there is little indication that it will extend meaningfully to the area of regulation relevant to this paper: cybersecurity.

The United States' asymmetrical nonregulatory attitude has contributed to weak cybersecurity in the United States, since it has meant that the US government has generally failed to clamp down on some of the many cybersecurity harms generated by US firms. This hesitation to regulate takes many guises—the absence of software

liability or regulation for contributions to cyber losses, the general failure to impose significant liability on firms that suffer significant data breaches, the hesitation to require or facilitate better information-sharing requirements, the absence of mandated (or at least subsidized or incentivized) security measures such as encrypted connections to websites or physical security tokens for authentication, and the like.

We do not here advocate any particular regulatory measure, and it is hard to generalize about the extent to which US adversaries are more interventionist in these cybersecurity contexts. Our only point is that to the extent US adversaries face no ideological or cultural opposition to such intervention, this yields a potentially significant cybersecurity advantage in defending their systems.

VIII. Conclusion

The United States' global economic dominance, its digital depth, its commitment to free speech and a free press and the rule of law, its relatively transparent government, and its relative regulatory skepticism, have long been defining and proud characteristics of its strength. In this essay, we have argued that, in the digital era, these defining strengths create structural downsides for the United States compared to its adversaries, especially authoritarian ones. Some of these characteristic strengths can of course be exploited by adversaries in nondigital realms. But as we have tried to show, digitalization significantly exacerbates the asymmetrical downsides of these constitutive elements of US power and creates special opportunities for foreign adversaries.

We cannot measure the scale of these downsides for the United States, nor can we balance the downsides against the many benefits of digitalization for the United States in its international relations. Any serious effort at assessing the impact on the asymmetries we have identified would need to grapple with the relationship among the United States' various forms of power, and with it complex interdependencies with other nations.[55] This and many other confounding factors are why we do not hazard any predictions about the aggregate impact on US international relations from the asymmetries and downsides we have identified.

And yet we do think there are reasons to be pessimistic. First, it is clear that the United States is incurring significant damage on many dimensions vis-à-vis its authoritarian adversaries as a result of the asymmetries we have identified. These are losses that it either did not suffer, or did not suffer at nearly the same scale, prior to the digital revolution. Second, the United States appears to have no feasible plan to redress, or even a theoretical response to, most of the asymmetrical downsides to digitalization

that we have identified. The problem of digital theft might smooth out over time. And in many bilateral relationships, digital dependence might be symmetrical and thus a less severe problem for the United States. But even viewing those issues optimistically, the problems for the United States that arise from its commitment to free speech and a free press and to certain legal constraints, and from its relatively transparent government and relative regulatory skepticism, have no great solution on the horizon.

Moreover, if we step back from the daily public reports of cyber operations against the United States and look at the broader picture—at least the picture one can form based on publicly available information and on the near-despairing comments by US officials—matters seem to be getting progressively worse. The number of cyber operations against the United States is growing, and the losses in various dimensions are mounting.

We have tried in this paper to explain some of the structural reasons why the United States might be especially ill-suited to respond to or deal with the soft cyber operations that have done the vast majority of the damage. One would like to think that we will soon see an equilibrium point where the losses will stabilize due to countervailing pressures. But given the deep structural asymmetrical basis for the losses, and the relative ease with which a growing number of adversaries can continue to impose these losses, that stabilization point is hard to see or even imagine at the moment.

Acknowledgments

For helpful comments, we thank Gabriella Blum, Ben Buchanan, Richard Danzig, Adam Klein, Herb Lin, Matt Noyes, Joseph Nye, Michael Sulmeyer, and participants at workshops at Columbia and NYU law schools and at the Belfer Center's Cyber Security Project. For helpful research assistance, we thank Rishabh Bhandari and Andrei Gribakov.

NOTES

1 Benjamin Wittes and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones; Confronting a New Age of Threat* (New York: Basic Books, 2015), 177–79. Wittes and Blum use the Roman road analogy to make the point that "new technologies of mass empowerment," including digital systems, "create new security issues that, left unaddressed, leave the platform unsafe for use and potentially threatening to the society that created it" (180).

2 For good discussions of the difficulties of prediction in this and related contexts, see Philip Tetlock, *Expert Political Judgment* (Princeton: Princeton University Press, 2006); and Richard Danzig, "Driving in the Dark: Ten Propositions about Prediction and National Security" (Center for a New American Security, October 2011).

3 All but the last two items on this list are typically categorized by the Defense Department as "computer network exploitations," while the last two items are typically categorized as "computer network attacks."

4 Kristin Stoller, "The World's Largest Tech Companies 2017: Apple and Samsung Lead, Facebook Rises," *Forbes*, May 24, 2017, accessed May 23, 2018, https://www.forbes.com/sites/kristinstoller/2017/05/24/the-worlds-largest-tech-companies-2017-apple-and-samsung-lead-facebook-rises/#3b59322ed140.

5 Tim Bradshaw, "Tech World's 'Fearsome Five' Top Most Valuable Brands List," *Financial Times*, June 5, 2017.

6 On soft power in the cyber realm, see Joseph S. Nye Jr., "Cyber Power" (Belfer Center, May 2010), accessed May 23, 2018, https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf. See also Olivia Solon and Sabrina Siddiqui, "Forget Wall Street—Silicon Valley Is the New Political Power in Washington," *Guardian*, September 3, 2017, accessed May 23, 2018, https://www.theguardian.com/technology/2017/sep/03/silicon-valley-politics-lobbying-washington.

7 Joe Uchill, "Obama: US Government Has Largest Capacity to Hack," *The Hill*, September 6, 2016, accessed May 23, 2018, http://thehill.com/policy/cybersecurity/294572-obama-us-has-largest-cyber-capacity.

8 See Section 702 of the Foreign Intelligence Surveillance Act (FISA), 50 US Code § 1881a.

9 We elaborate on many of these points in more detail below. For a more extended explanation, see Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Center for a New American Security, July 2014), accessed May 23, 2018, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf?mtime=20161010215746; and Joseph S. Nye Jr., "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 19–22.

10 Josh Rogen, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" *Foreign Policy*, July 9, 2012, accessed May 23, 2018, http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history.

11 See Adam Rawnsley, "Espionage? Moi?," *Foreign Policy*, July 2, 2013, accessed May 23, 2018, http://foreignpolicy.com/2013/07/02/espionage-moi; and Melanie Reid, "A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat?," *University of Miami Law Review* 70 (2016): 797–98.

12 Alyssa Abkowitz, "The Cashless Society Has Arrived—Only It's in China," *Wall Street Journal*, January 4, 2018.

13 This is a standard feature of uneven global economic development. In the nineteenth century, US firms frequently stole intellectual property from British firms and authors. See, e.g., Mike W. Peng, David Ahlstrom, Shawn M. Carraher, and Weilei Stone Shi, "History and the Debate over Intellectual Property," *Management and Organization Review* 13, no. 1 (April 2017): 15–38.

14 "Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage," IC on the Record, September 8, 2013, accessed May 23, 2018, https://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence. The narrowness of the US commercial theft ban should be emphasized. A former CIA director has acknowledged that the US government "steal[s] secrets with espionage, with communications, with reconnaissance satellites" from "foreign corporations and foreign government's assistance to them in the economic area," in three "main areas": (1) to understand how sanctions regimes are operating; (2) to monitor dangerous dual-use technologies in private hands; and (3) to learn about bribery practices. See "Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage," statement by James Woolsey, former director, Central Intelligence Agency, Federation of American Scientists, March 7, 2000, accessed May 23, 2018, https://fas.org/irp/news/2000/03/wool0300.htm. The United States might also steal foreign commercial secrets for other reasons that can be used by the government to benefit the US economy and US firms. See Jack

Goldsmith, "The Precise (and Narrow) Limits on U.S. Economic Espionage," *Lawfare* (blog), March 23, 2015, accessed May 23, 2018, https://lawfareblog.com/precise-and-narrow-limits-us-economic-espionage. What the United States does not do, according to its policy, is steal information from foreign firms to give to particular companies to advance their competitiveness. According to unnamed US officials, "while the N.S.A. cannot spy on Airbus and give the results to Boeing, it is free to spy on European or Asian trade negotiators and use the results to help American trade officials—and, by extension, the American industries and workers they are trying to bolster." David E. Sanger, "Fine Line Seen in U.S. Spying on Companies," *New York Times*, May 20, 2014.

15 Another potential tool would be for the United States to steal the commercial information and publish it without giving it to any particular country. It is not clear why the United States does not do this, but it might have something to do with the vulnerabilities that come from digital dependence, as outlined in part III.

16 The White House, Office of the Press Secretary, "Fact Sheet: President Xi Jinping's State Visit to the United States," news release, September 25, 2015, accessed May 23, 2018, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

17 David E. Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds," *New York Times*, June 20, 2016.

18 See Jack Goldsmith, "China and Cybertheft: Did Action Follow Words?," *Lawfare* (blog), March 18, 2016, accessed May 23, 2018, https://www.lawfareblog.com/china-and-cybertheft-did-action-follow-words.

19 Mara Hvistendahl, "The Decline in Chinese Cyberattacks: The Story behind the Numbers," *MIT Technology Review*, October 25, 2016, accessed May 23, 2018, https://www.technologyreview.com/s/602705/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers.

20 FireEye iSight Intelligence, "Redline Drawn: China Recalculates Its Use of Cyber Espionage," June 2016, accessed May 23, 2018, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf; see also Jack Goldsmith, "U.S. Attribution of China's Cyber-Theft Aids Xi's Centralization and Anti-corruption Efforts," *Lawfare* (blog), June 21, 2016, accessed May 23, 2018, https://www.lawfareblog.com/us-attribution-chinas-cyber-theft-aids-xis-centralization-and-anti-corruption-efforts.

21 Office of the United States Trade Representative, Executive Office of the President, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," p. 168, March 22, 2018, accessed May 23, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF; see also Sam Kim, "China Hacks U.S. Firms for Financial Information, FireEye Says," *Bloomberg*, April 4, 2018, accessed May 23, 2018, https://www.bloomberg.com/news/articles/2018-04-04/china-hacks-u-s-firms-for-financial-information-fireeye-says (noting recent uptick in Chinese commercial cyber theft related to financial institutions).

22 On the themes in this paragraph, see Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010).

23 Tim Hornyak, "2014 Cyberattack to Cost Sony $35M in IT Repairs," *Computer World*, February 4, 2015, accessed May 23, 2018, https://www.computerworld.com/article/2879480/2014-cyberattack-to-cost-sony-35m-in-it-repairs.html.

24 David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 15, 2017.

25 Sanger, Kirkpatrick, and Perlroth, "The World Once Laughed."

26 Timothy W. Martin, "How North Korea's Hackers Became Dangerously Good," *Wall Street Journal*, April 19, 2018, accessed May 23, 2018, https://www.wsj.com/articles/how-north-koreas-hackers-became-dangerously-good-1524150416.

27 Sanger, Kirkpatrick, and Perlroth, "The World Once Laughed."

28 Sanger, Kirkpatrick, and Perlroth, "The World Once Laughed."

29 David E. Sanger and Nicole Perlroth, "What Options Does the U.S. Have after Accusing Russia of Hacks?," *New York Times*, October 8, 2016, accessed May 23, 2018, https://www.nytimes.com/2016/10/09/us/politics/what-options-does-the-us-have-after-accusing-russia-of-hacks.html; Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016, accessed May 23, 2018, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

30 Shaun Waterman, "Clapper: U.S. Shelved 'Hack Backs' due to Counterattack Fears," *CyberScoop*, October 2, 2017, https://www.cyberscoop.com/hack-back-james-clapper-iran-north-korea.

31 And more broadly, since the US foreign policy agenda is generally so much broader than that of other countries, the US government often faces unusually complex trade-offs when it comes to when and how, if at all, to retaliate against cyber operations (or any form of damaging foreign operation).

32 In addition to the events recounted above, see, for example, Nicole Perlroth, "Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks," *New York Times*, May 11, 2018, accessed May 23, 2018, https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html (former NSA director Keith Alexander states, concerning threats of Iranian cyberattacks: "We're probably one of the most automated technology countries in the world. . . . We could have a very good offense, but so do they. And unfortunately, we have more to lose").

33 Indeed, the Trump administration's Nuclear Posture Review announced a broad declaratory policy of using nuclear weapons to deter nonnuclear threats. See Department of Defense, Nuclear Posture Review (2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-nuclear-posture-review-final-report.pdf.

34 See Joseph Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 44–71.

35 For the history of this view and its early repudiation, see Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2008).

36 See, generally, Nathalie Maréchal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communication* 5, no. 1 (2017): 29–41, accessed May 23, 2018, https://www.cogitatiopress.com/mediaandcommunication/article/view/808/808; and K. Ognyanova, "Careful What You Say: Media Control in Putin's Russia; Implications for Online Content," *International Journal of E-Politics* 1, no. 2 (2010): 1–15.

37 Barack H. Obama, news conference, December 16, 2016, accessed May 23, 2018, http://www.presidency.ucsb.edu/ws/index.php?pid=119865.

38 David M. Herszenhorn and Ellen Barry, "Putin Contends Clinton Incited Unrest over Vote," *New York Times*, December 8, 2011.

39 Reuters, "U.S. Authorities Identify Six Russian Officials in DNC Hack: WSJ," November 2, 2017, accessed May 23, 2018, https://www.reuters.com/article/us-usa-trump-russia-hackers/u-s-authorities-identify-six-russian-officials-in-dnc-hack-wsj-idUSKBN1D21MI.

40 Jessie Hellmann, "Putin: Panama Papers Leak Are a US Plot to Weaken Russia," *The Hill*, April 7, 2016, accessed May 23, 2018, http://thehill.com/blogs/blog-briefing-room/news/275510-putin-panama-papers-leak-are-a-us-plot-to-weaken-russia.

41 For various accounts, see Foreign Policy Association, "Putin Emerges as a Winner in the Panama Papers Scandal," *Foreign Policy Blogs*, April 28, 2016, accessed May 23, 2018, https://foreignpolicyblogs.com/2016/04/28/putin-emerges-winner-panama-papers-scandal; "Panama Papers: How Moscow and Beijing Reported Panama," BBC, April 4, 2016, accessed May 23, 2018, http://www.bbc.com/news/world-35959855; Martin Armstrong, "Putin's Approval Rating High Despite Protests," Statista, June 12, 2017, accessed May 23, 2018, https://www.statista.com/chart/9772/putins-approval-rating-high-despite-protests.

42 For an example of trumpeting success, see Mark Pomerleau, "Carter Looking to Drop 'Cyber Bombs' on ISIS," *Defense Systems*, February 29, 2016, accessed May 23, 2018, https://defensesystems.com/articles/2016/02/29/dod-carter-isis-cyber-bombs.aspx (Secretary of Defense Ashton Carter stating, "We are using cyber tools, which is really a major new departure. I'm talking about attacking the ability of someone sitting in Raqqa to command and control ISIL forces outside of Raqqa or to talk to Mosul. Or even to talk to somebody in Paris or to the United States. So these are strikes that are conducted in the warzone using cyber essentially as a weapon of war just like we drop bombs. We're dropping cyber bombs.").

43 For a recent episode, see Scott Shane and Adam Goldman, "Suspect Identified in C.I.A. Leak Was Charged, but Not for the Breach," *New York Times*, May 15, 2018 (identifying the former CIA software engineer responsible for the largest loss of classified documents in CIA history).

44 Compare Richard Helms, *A Look over My Shoulder: A Life in the Central Intelligence Agency* (Novato: Presidio Press, 2003), 184–85 (noting that "the probability of leaks escalates exponentially each time a classified document is exposed to another person—be it an Agency employee, a member of Congress, a senior official, a typist, or a file clerk").

45 Jack Goldsmith, "Extraordinary U.S. Press Freedom to Report Classified Information," *Lawfare* (blog), December 2, 2013, accessed May 23, 2018, https://www.lawfareblog.com/extraordinary-us-press-freedom-report-classified-information.

46 Ellen Barry, "Russian Ex-Spy Sergei Skripal Was Poisoned via Front Door, U.K. Says," *New York Times*, March 28, 2018.

47 Compare Benjamin Edwards, Alexander Furnas, Stephanie Forrest, and Robert Axelrod, "Strategic Aspects of Cyberattack, Attribution, and Blame," *Proceedings of the National Academy of Sciences* 114, no. 11 (March 14, 2017): 2825–30, accessed May 23, 2018, http://www.pnas.org/content/pnas/114/11/2825.full.pdf.

48 See, generally, Jack Goldsmith, *Power and Constraint: The Accountable Presidency after 9/11* (New York: W. W. Norton & Company, 2012).

49 See Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

50 See National Security Act, 50 U.S.C. § 3093(f); see also United States Intelligence Activities, Executive Order 12333, Section 2.13.

51 These operations are akin to the espionage, propaganda, electoral influence, and black bag jobs that nations have long practiced in the predigital era, though their frequency and effects are amplified significantly due to digitalization. The low-level cyber operations are either not regulated by international law, are affirmatively permitted by it, or at least are not obviously prohibited by it.

52 Waterman, "Clapper."

53 There might be good policy reasons for the restraint about violating third-country sovereignty in the cyber context, such as a concern that third parties might use infrastructure on US soil as a channel of

attack in a third country, and a belief that restraint by the United States in this context will constrain its adversaries in doing the same thing to it. To the extent this is true, constraint abroad related to sovereignty might be grounded as much in digital dependence as in legal constraint. But in public accounts, policy makers have emphasized legal restraint, which is clearly in play and consequential compared to adversaries.

54 Waterman, "Clapper."

55 See Robert O. Keohane and Joseph S. Nye Jr., *Power and Interdependence* (New York: Pearson, 1977).

The preferred citation for this publication is Jack Goldsmith and Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations,* Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1806 (June 5, 2018), available at https://lawfareblog.com /strengths-become-vulnerabilities-how-digital-world-disadvantages-united-states-its-international-0.

About the Authors

STUART RUSSELL

Stuart Russell is a visiting fellow at Harvard Kennedy School's Belfer Center where he works on the Cyber Security Project. Stuart is on loan from the UK Government where he has worked in a range of roles covering technology, cybersecurity, and national security. His research focus is on the interplay between cybersecurity, privacy, and national security. Stuart holds a Master's degree in Physics and Astronomy from the University of Durham, UK.

JACK GOLDSMITH

Jack Goldsmith is the Henry L. Shattuck Professor at Harvard Law School, a Senior Fellow at the Hoover Institution, and cofounder of *Lawfare*. He teaches and writes about national security law, presidential power, cybersecurity, international law, Internet law, foreign relations law, and conflict of laws. Before coming to Harvard, professor Goldsmith served as Assistant Attorney General, Office of Legal Counsel from 2003 to 2004, and Special Counsel to the Department of Defense from 2002 to 2003.

Working Group on National Security, Technology, and Law

The Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the Lawfare blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith and Benjamin Wittes are the cochairs of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
The Johnson Center
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION