Divide and Rule

Republican Security Theory as Civil Society Cyber Strategy

Ronald Deibert

The Edward Snowden National Security Agency (NSA) revelations have touched off soul-searching discussions in the United States about the legality of mass surveillance programs; in particular, whether they violate the Fourth and Fifth Amendments of the U.S. Constitution, and whether proper oversight and accountability exist to protect citizens’ rights. They have also cast into stark relief tensions in U.S. rhetoric and practice, the most obvious of which is the disconnect between the operations of the National Security Agency and the American-led Internet Freedom agenda. As regimes in the global South begin to piece together the hidden mechanisms of structural information power, arguments for an “open Internet” will face an uphill battle against pressures to subject cyberspace to greater sovereign controls.¹ While the United States is most in the spotlight, other liberal democratic countries share the same contradictions, especially as growing curiosity and further revelations bring to the surface their own secretive surveillance programs.² These contradictions underscore the tensions between a globally distributed information and communications space layered on top of the Westphalian state system with all its competitive power dynamics.

¹
²

Ronald Deibert is a professor of Political Science and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Monk School of Global Affairs at the University of Toronto. He is also a co-founder and a principal investigator of the Open Net Initiative and Information Warfare Monitor (2003–2012) projects.
As cyberspace has become the infrastructure for global communications, the security of the domain has become a top priority. Yet, rarely examined directly are the questions, security for whom and security for what? Although engineers like to think of cyber security as a technical problem requiring a “fix” or “patch,” security is always for someone and some purpose and is, therefore, always inherently political.

In the absence of considered alternatives, the tendency has been to default to the Realist approach to statecraft and all that it entails. Not surprisingly, we are seeing reflexive policies that involve erecting defensive perimeters to the world outside; solutions that depend on hierarchy, secrecy, and classification; and defense and intelligence agencies taking on leading roles. These approaches result in the gradual erosion of checks and balances on power, self-reinforcing cycles of hostility and suspicions abroad, and a dangerously escalating arms race in cyberspace fuelled by a growing cyber security industrial complex.

In his book, *Black Code*, this author has argued that in the headlong rush to security, liberal democratic countries are losing sight of that which they should be securing in the first place: a robust system of checks and balances that, supported by the free flow of information and commerce, cuts across domestic and international divides of like-minded countries and gradually results in the integration of security communities sharing a commitment to the rule of law and human rights. Part of the problem rests with the communities most dependent on the success of such a vision: global civil society. Those who would consider themselves to be part of global civil society have been among the most persistent watchdogs of governments and corporations, spotlighting violations of human rights online, and calling out surveillance and censorship. However, they have found it much easier to identify what they are against than what they are for, especially when it comes to securing cyberspace. Security is traditionally seen as an anathema to civil society, for some the language itself evocative of the very constituencies that need to be resisted. Yet, sidestepping the conversation will ensure only that citizens communicate in environments secured according to the interests and values of others. Civil society is moreover critically dependent on communications, and should see securing cyberspace as a top priority as much as any other stakeholder.

To be sure, what is loosely called “global civil society” is hardly unified, and contains many divisions along ethnic, gendered, and regional lines. However, at a baseline, all of civil society depends on both an open and secure Internet, one not subject to disruption and through which ideas can be freely exchanged by citizens around the world. In the following article, the author lays out what he believes some of the core elements of that strategy should be, beginning with a consideration of first principles. Together these strategies are oriented around building a fortress for liberal democratic republics that can be extended as part of a global civil society strategy for cyberspace.

Starting with First Principles. The political nature of security begins with what is defined as the “object” of
security, meaning that which is considered worth protecting. While the object of security in international affairs may seem too obvious to state, there is wide variation in objects of security, even in today’s nation-state system. For some, the object of security is the entire country: its population, territory, and way of life. For others, it is more narrowly defined around the regime, party, or even an individual in power.

It is remarkable how rarely such considerations of first principles around security are examined. Part of the reason is that for so long, one tradition has had a monopoly on security discourse and practice. Once invoked, security tends to privilege Realist-associated institutional responses and elevate certain priorities in an almost instinctual fashion: hierarchy, secrecy, concentration of power, the erection of borders between “inside” and “outside,” and the employment of military and intelligence agencies to positions of power and authority. While these lessons have a long pedigree and were formed out of centuries of hard-fought experiences, they may not always be appropriate to the conditions of a time and place.

There is also a lack of clearly articulated alternatives to this tradition, especially in civil society. Not surprisingly, those who consider themselves to be part of a global civil society, such as advocates of human rights, lack their own tradition of security from which to draw. Security tends to be seen by members of this community as something to be resisted at best, or delegated to the men and women in uniform at worst. Those among civil society who are outraged today by revelations of government surveillance may even go further, believing that no government is good government. Yet, civil society is inherently dependent on the rule of law, without which human rights—including privacy, freedom of speech, and access to information—cannot be guaranteed. Without agencies capable of enforcing laws or defending against those whose aims are to destroy the very basis of liberal democracy, civil society networks would quickly find themselves extinguished. It is both undesirable and unrealistic to advocate doing away with government altogether. The question is not a matter of states versus no-states, but rather which type of state do we want?

In prior publications, the author has drawn from the work of Johns Hopkins University Professor Daniel Deudney to argue that there is a long-standing security theory at the heart of liberal democratic thought, one which is derived from the republican tradition of politics stretching to ancient Greece. While having different elements, that tradition can be boiled down to core practices that mix and disperse authority around a system of checks and balances, in order to tie down and prevent the concentration of political power. Deudney has described these republican security practices as employing the structural principle of “negarchy,” namely, something in between the twin evils of anarchy and hierarchy.

Republican security thinking is associated mostly with domestic political orders, but it is inherently an international approach as reflected in the founding of the early United States of America and later the European Union, both of which sought to achieve a confederation of independent units.
but stopped short of full amalgamation into a consolidated state. Republican systems of rule are designed to guard against not only internal hierarchy, but also external predation and empire. Republican strategies seek to reign in other states in federalist arrangements, essentially broadening the umbrella of political jurisdictions that are subject to the same principles of mixture, division, and restraint. Republican security theory rests on the assumption that when governments are tied down into clearly defined, federated channels of cooperation, a multitude of lower-level transnational flows of people, commerce, information, and ideas will flourish and provide buttresses to the deepening of zones of liberal peace.

Reflecting on this theory in the context of cyberspace governance, it is noteworthy that the Internet exploded in a short period to become one of the most densely integrated of these transnational networks. However, the gradual encroachment of governments into Internet policy has imposed borders on cyberspace, perversely undermining one of the pillars of republican security practice in the process. More than forty countries engage in some form of Internet censorship, including liberal democratic countries, with the censorship undertaken in secrecy using technologies developed by Western firms. The NSA scandal will almost certainly deepen these territorializing tendencies as countries seek to rectify the perceived dependence on American-owned infrastructures that give the United States a distinct "home field" advantage. Countries that aim to impose greater border controls on cyberspace are now focusing on shaping technical standards, requiring companies to design into their systems lawful "back doors," or looking to create national alternatives to foreign products and services that can be subject to local laws.

Countering these tendencies requires a nuanced understanding of the interconnections between these multi-layered processes, and an orientation starting with first principles and working outwards. From this perspective, speaking about "Internet freedom" abroad while taking advantage of locally domiciled companies to subject communications to surveillance seems like self-serving hypocrisy. Instead, it is in the interest of liberal democratic governments to push for ever expanding transnational communications infrastructures that operate with the greatest degree of transparency and independence from specific jurisdictions, while working to strengthen and deepen practices of mixture, division, and restraint starting in the liberal democratic core and working outwards.

From this perspective, speaking about "Internet freedom" abroad while taking advantage of locally domiciled companies to subject communications to surveillance smacks of self-serving hypocrisy.
Building Transnational Epistemic Communities around Cyber Security. Of course, the world is a dangerous place and there are many who seek to exploit vulnerabilities in cyberspace to undermine liberal democracy. When it comes to policing cyber security threats—such as botnets, malware, and threats to critical infrastructure—distributed security provides a model for the enhancement of the best parts of existing practice. Today, the Internet functions remarkably well largely because of transnational networks of engineers—the security community—who works on the basis of reputation and trust. Most of the members of this distributed security community come from the private, non-profit, advanced research, and civil society sectors. Instead of replacing these communities with a top-down, state centric approach, and a philosophy that embraces offensive computer network attacks as a deterrent (both of which are contrary to the constitutive principles of the Internet), one should find ways to support and expand these distributed networks.¹⁰ Building resilience into the design of cyberspace begins with empowering locally rooted but highly connected experts.

While the individuals who make up these distributed security communities may not be able to recite Polybius, Montesquieu, or Publius, their operating norms are the fullest expression of republican security thinking in practice, an example of “networked governance,” which Mueller, Schmidt, and Kuerbis, describe as “a semipermanent, voluntary negotiation system that allows interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority.”¹¹ In the cyber security domain, this type of networked governance is apparent in the cooperation among national computer emergency response teams (CERTS), which have grown and become more deeply entrenched over time and supported through fora like the Forum of Incident Response and Security Teams (FIRST) and processes like the London Action Plan.¹² According to Mueller et al., networked governance is also evident in the most basic process of the Internet, that which concerns Internet routing of autonomous systems (ASs).¹³ As they describe, “[m]ultiple operators of ASs coordinate their actions to produce global connectivity, but each one is free to define its own policies and make its own decision about what other operators’ routing announcements are and which packets it will accept or reject.... Routing policies and practices as a whole are not subject to the hierarchical regulation of a single authority.”¹⁴

Borrowing language from International Relations theory, these networks very much resemble epistemic communities; that is, networks of professionals with recognized knowledge and technical skills around a particular issue-area.¹⁵ Transnational epistemic communities, including the cyber security community, influence politics through technical standard setting, diffusing knowledge through systems of trust and reputation, and largely immunize their decisions from national political rivalries. Critical to the success of these networks is the peer system, both in terms of relying on reputation and trust for continued operational success, and in organization along non-hierarchical
lines very much in concert with the distributed approach to security. Over time, the autonomy of these networks has subtly eroded, and hierarchical elements have been gradually introduced. Technical governance and standard setting forums have become increasingly politicized, as the stakes have become higher and governments have intervened. National law enforcement and intelligence agencies are not only more present at the Internet technical and standard setting forums, but they are also playing a more influential role in response to cyber security policing. Studies of botnet takedowns, for example, show growing law enforcement and government participation. While networked, peer production governance of cyber security has not been entirely overturned, the general trend is towards more state involvement, hybrid forms of networked-hierarchical practices, growing secrecy, and politicization of technical standards.

A republican cyber security strategy would seek to reverse this process, immunizing cyber security epistemic communities from national rivalry while building out the local capacities of these fora across global regions, extending peer security production, and then shielding the network from co-optation by partial state or corporate interests. Although law enforcement participation in cyber security policing is largely unavoidable, and even desirable, these agencies should be constrained as peers in a network, rather than superordinate officials in a hierarchy. Setting the norms around how policing takes place in cases like botnet takedowns is exceptionally important. Here, liberal democratic governments have a pro-active role to play in actually limiting their own involvement and explicitly protecting the autonomy of these fora, while discouraging other states from throwing their political weight around. The networked governance around cyber security is a critical element of the republican security approach and should be extended as part of a civil society cyber security strategy.

Opening Up the Black Box. At the heart of republican security practices is what Jeremy Bentham called a “system of distrust,” one in which elites are kept in line, in part, by fear of public exposure. Likewise, John Stuart Mill argued that exposure compels “deliberation and force[s] everyone to determine, before he acts, what he shall say if called to account for his actions.” Government secrecy in a liberal democracy should be practiced infrequently with exceptional justifications, and closely monitored by independent oversight bodies.

Over the years, however, and especially in response to the exigencies of 9/11, government secrecy has ballooned. Ironically, at the same time that many
elected officials have been campaigning on platforms of “open government,” security programs are being quietly buried in layers of classification and shielded from public scrutiny. For example, the deliberations of the U.S. court whose ostensive mission is to provide a check against the operations of the NSA, the Foreign Intelligence Services Court, are themselves shielded from public scrutiny. At the same time, government agencies that operate with the most secrecy, notably signals intelligence, have mushroomed in scope and scale, their budgets and missions expanding. The influence of these programs has extended into the private sector, including scores of defence and intelligence contractors that service their programs, like Edward Snowden’s former employer Booz Allen Hamilton. These companies are drawn into an orbit of classification and secrecy. By some estimates, as many as 1.4 million Americans hold Top Secret clearances.\textsuperscript{17}

While a great deal of attention has focused on the adequacy of the United States system of checks and balances in the wake of the Snowden revelations, arguably its system of oversight is much more rigorous than those of other liberal democratic countries. In Canada, for example, the operations of the Communications Security Establishment of Canada (CSEC)—the Canadian counterpart to the American NSA—are overseen by a single independent commissioner, a retired federal judge. There is no parliamentary oversight of the CSEC. Meanwhile, its budget and staff have grown considerably since 2001. Likewise, recent reports by the Guardian disclosed that officials in the U.K.’s Government Communications Headquarters (GCHQ) held the belief that “[W]e have a light oversight regime compared with the US.”\textsuperscript{18}

Not only have these agencies ballooned in size, but some have also been given expanded responsibilities as lead agencies in cyber security. For example, the NSA and the U.S. Cyber Command share the same chief, General Keith Alexander. According to intelligence historian James Bamford, “[n]ever before has anyone in America’s intelligence sphere come close to his degree of power, the number of people under his command, the expanse of his rule, the length of his reign, or the depth of his secrecy.”\textsuperscript{19} More important than Alexander’s personal rule, however, is the gradual positioning of the NSA as the command agency for U.S. cyber security. While it certainly can make an argument for having the most advanced capabilities for the mission, the secrecy that surrounds the organization means that having it do so can further international suspicion, undermine international cooperation, and introduce military solutions to a domain that is primarily owned and operated by the private sector.

A corrective to this excess should be an urgent priority, and a good place from which to start are the Tshwane Principles, drafted by 22 organizations and academic centers in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world. The principles recognize that withholding information from the public is often a necessary component to protect the full exercise of human rights. However, they affirm that the requirements for restricting
the right to information on national security grounds must meet at a minimum the following criteria:

No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts.

The report also stresses that “[a] government’s over-invocation of national security concerns can seriously undermine the main institutional safeguards against government abuse: independence of the courts, the rule of law, legislative oversight, media freedom, and open government.” Intelligence agencies are still essential to the security of liberal democracy in a dangerous world. Yet, in the headlong rush to deal with serious threats, the pendulum has swung too far away from basic mechanisms of oversight and accountability, risking the very real possibility of the abuse of concentrated power in the hands of a few public officials. Rectifying this imbalance is an essential component of republican security practice.

**Shutting the Back Door.** The prevailing paradigm of cyber security has brought about pressures on industry not only to provide governments with access to data they control, but also to build directly into their technologies access systems, known as “backdoors.” Built-in backdoors for law enforcement and intelligence agencies are not new to the post 9/11 era. The so-called “Clipper Chip” debate of the 1990s was very much centered on the wisdom and utility of providing the U.S. government with special access to encryption systems. While critics of the Clipper Chip managed to scuttle those proposals, the same basic back door mechanism has persisted and grown widely as concerns around cyber security have grown. Recently, for example, the Federal Bureau of Investigation (FBI) has lobbied extensively for back door mechanisms, arguing that it risked “going dark” without new wiretapping capabilities. In light of the revelations about NSA and FBI wholesale data collection programs, including bulk collection of metadata, the concerns seem ludicrous; indeed, a more persuasive case could be made that members of the public live in golden age of surveillance, and the greatest risk for law enforcement is not too little, but rather too much data.

Quite apart from the merits of the argument on its own terms, however, is a very specific concern about security. Building backdoors into devices and infrastructure may be useful to law enforcement, but they also provide a built-in vulnerability for those who seek to exploit them. For example, in 2008, Citizen Lab researchers discovered that the Chinese version of the popular VOIP product, Skype (called TOM-Skype), had been coded with a special surveillance system in place such that whenever certain keywords were typed into the chat client, data would be sent to a server in mainland China (presumably to share with China’s security services). Upon further investigation, experts discovered that the server onto which the chat messages were stored...
was not password protected, allowing one to download millions of personal chats that included credit card numbers, business transactions, and other sensitive information. Some reports indicate that the China-based espionage attacks aimed at Google and other companies were focused on Google’s lawful access backdoor systems, now known by the code-name PRISM. In framework, have security implications insofar as they restrict the volume of stored data that might be exploited for nefarious purposes. In a world of “Big Data,” in which so much of our information is routinely given away as part of our daily life, law enforcement and intelligence agencies need to find ways to work within this universe as it exists, rather than drill holes from the inside-

Building backdoors into devices and infrastructure may be useful to law enforcement, but they also provide a built-in vulnerability for those who seek to exploit them.

2013, a team of twenty computer security researchers issued a report published by the U.S.-based Center for Democracy and Technology, arguing that “mandating wiretap capabilities in endpoints poses serious security risks,” and that building “intercept functionality into... products is unwise and will be ineffective, with the result being serious consequences for the economic well-being and national security of the United States.”

Rather than building in such insecurities by design, a republican cyber security strategy would emphasize the opposite: encouraging the widespread use of the state of the art encryption, the adoption of standards such as “https by default” and “two factor authentication,” and the promotion of open source software to build confidence across borders. In line with this approach would be regulations around deletion of stored data and proposals like the “right to be forgotten,” which, although typically seen in a rights-based framework, have security implications insofar as they restrict the volume of stored data that might be exploited for nefarious purposes. In a world of “Big Data,” in which so much of our information is routinely given away as part of our daily life, law enforcement and intelligence agencies need to find ways to work within this universe as it exists, rather than drill holes from the inside-

Privacy as Cyber Security. Paradoxically, the powers and capabilities of security agencies are being expanded at the very same time that members of the public are effectively turning their digital lives inside out. Every individual now gives away endless streams of data about his or her personal life; social networks; tastes and preferences; and even physical location into both the public domain and also the hands of third parties. This fundamental change in the material conditions of cyberspace has dramatically altered the constraints and opportunities for surveillance. But corresponding changes in privacy and other data protections have not kept pace.

Privacy is a basic human right set out in Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the
Universal Declaration of Human Rights (UDHR). Yet, for too many it is seen as an afterthought, already sacrificed in the onrush of social networking, mobile connectivity, and cloud computing. Arguably, a case could be made that the powers, capabilities, and scope of privacy commissioners and relevant data protection laws should be expanded at least as much, if not more, than security agencies, not only as a bulwark for privacy, but also more broadly as a critical component of distributed cyber security. With so much information entrusted to or otherwise shared with scores of third parties, many of them operating in multiple national jurisdictions, there is a pressing need to ensure the secure handling of that data.

While the American model has relied on patchwork rules and regulations, the European, Canadian, and other models rely more on privacy commissioners who are given independent power and investigative capabilities to act as a watchdog on both governments and corporations. Enhancing these powers would also act as a check against insecurities that might arise from poor data handling practices that in turn lead to further breaches and insecurities. Strong privacy commissioners should be granted independent power to ensure that governments and corporations practice data minimization, purpose limitation, limited storage periods, and notification procedures to customers and citizens, particularly with regard to the transfer of data to third parties or other political jurisdictions than those in which a citizen has rights.

Multi-Stakeholderism: Where’s the Beef? Leading up to and during the International Telecommunications Union’s World Conference on International Telecommunications (WCIT) summit in Dubai, governments polarized around those who supported a greater role for governments in Internet governance, and those who support the “multistakeholder” model. Often paid lip service, but rarely practiced fully by the governments who most ostensibly support it, the multistakeholder model is at risk of becoming what Claude Levi-Strauss once called “an empty signifier”—that is, a concept without any real object or referent. For example, the so-called London Process, which began in London in 2011, followed by Budapest (2012) and South Korea (2013), has been a state-led exercise, with civil society participants largely relegated to the margins and even excluded from meetings in which sensitive topics around security have been discussed. Should the London Process ever succeed, the outcome will likely very much reflect the interests of the participants as well as the lowest common denominator that unites China, Russia, the United States, and the United Kingdom.

The distributed security model, and in particular principles of mixture and division at the heart of it, give richer substance to the multi-stakeholder concept. According to this model, no one actor should be able to monopolize cyber security governance, and no decision can be undertaken without the participation and consent of all relevant stakeholders. With this model in mind, liberal democratic governments should ensure not only that civil society and
local Internet businesses are included in governance forums, but that they are integral to the policy processes leading up to them. Undoubtedly, such a shift in practice will cause some level of discomfort, as policy bureaucrats are not accustomed to extensive and continuous outreach. Yet, in the long run, these efforts will help support the greatest current threat to Internet freedom: the gradual encroachment of governments.

Conclusion. These elements of a republican strategy for cyber security are only starting points.25 Most of them are hardly novel, and each in their own right have been widely and loudly advocated by many organizations and individuals. However, it is important to remind oneself occasionally that the whole is greater than the sum of its parts; tying each of these elements together (and no doubt others that the author has failed to include here) into a coherent strategy will provide support, coherence, and direction to what otherwise might be seen as isolated arguments. Civil society need not shy away from the cyber security debate. Indeed, there is a rich tradition of republican theorizing about security from which to draw that can help inform a robust alternative to the conventional Realist approaches dominating today. The recent NSA revelations offer an opening to make such an argument, and to push for practical solutions to widespread cyber security issues from a republican security point of view.

NOTES
7 Frank La Rue, “Report of the Special Rappor-


22 Peter Swire and Keesa Ahmad, "'Going dark’ versus a ‘golden age of surveillance,” Center for Democracy and Technology, 2011.

