Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

Taking Care: Four Takes on the Cyber Steward

Roger Hurwitz

Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

March 18, 2012

This material is based on work supported by the U.S. Office of Naval Research, Grant No. N00014-09-1-0597. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

Citation: Hurwitz, R. (2012). Taking care: Four takes on the cyber steward. *Proceedings of the CyberDialogue 2012: What is Stewardship in Cyberspace?*

Unique Resource Identifier: https://cyberdialogue.ca/wp-content/uploads/2012/2012papers/CyberDialogue2012_hurwitz.pdfhttps://cyberdialogue.ca/previous-dialogues/2012-about/papers/

Version: Final published version.

TAKING CARE:
Four Takes on the CYBER STEWARD

ROGER HURWITZ

Computer Science and
Artificial Intelligence Laboratory, MIT

MARCH, 2012

CYBERDIALOGUE2012

WHAT IS STEWARDSHIP IN CYBERSPACE?

Canada Centre for Global Security Studies

MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

Stewardship denotes a custodial, non-proprietary relationship to a resource or domain. The notion of a "cyber steward" resonates with those of us who regard cyberspace as a commons or domain that belongs to no one, and yet we sense some duty to protect or manage it. This essay explores possible job descriptions of "cyber steward" and what might motivate a person or organization to take the job. The job description can vary with one's view of the commons. The motivations towards this stewardship usually involves more than the self-interested, prudential concern for future use of the commons, which drives self-organization to preserve natural resource commons. It can also involve more than a desire to reciprocate for the benefits now being enjoyed, as in the gift culture that marked the early days of the Internet. The "sense of duty" might answer to the interdependence of being in cyberspace, respond to a fear for the loss of its freedom, or harbour a utopian vision of a global society enabled by cyber networks. But it can also be a self-serving pretext to shield a ruling elite from criticism or to preserve some technological advantage over others.

TAKE 1: THE COMMONS AND THE STEWARD

A decade ago, Lawrence Lessig distinguished two cyber commons in a layered network model.[1] The first is the code or protocols at the middle layer, which by design enables the free flow of electronic packets from end-to-end (producer to consumer), regardless of the packets' contents or owners. With respect to the unfettered flow, the code layer is similar to other commons, such as the open seas and international airspace, where rights of passage are assured by traditions or agreements.[2] The code layer is additionally a commons in being open to innovation—people can build their own applications on top of it. The second cyber commons is in the content layer atop the code layer. It is composed of applications code and information that can be accessed without cost. Lessig noted that not all content there was free, much was copyrighted, but there were continuing efforts like file sharing, the Free Software Movement, and the Creative Commons to build a cultural commons.

Importantly, he acknowledged that these commons resulted from social choices, rather than inevitably from the technology. The end-to-end design at the code layer became feasible in the United States once court decisions had dissolved the old AT&T's control of the telephone networks and its restraint on innovation in services and devices. Such choices could be reversed: indeed the campaigns by the Recording Industry Association of America (RIAA) and Motion Pictures Association of America (MPAA) for draconian restrictions on fair use of purchased music and movies would produce one such reversal. Metaphorically put, these companies sought state aid to "enclose" parts of the cultural commons and keep it closed to free access.

1 Lawrence Lessig, "The Internet under Siege," Foreign Policy, November-December (2001): 56-65, http://lessig.org/blog/ForeignPolicy.pdf.

2 See for this analogy Abraham Denmark and James Mulvenon (eds.), Contested Commons: The Future of American Power in a Multipolar World (Washington, DC: Center for a New American Security, 2010).

The state's key role in enclosure is further seen by comparing the results of various organizations' "walled garden" strategies. In market-organized societies, such strategies restrict the applications (or information) that can run on a company's platforms, so it can command premium prices for its version of an application. America Online's (AOL) "walled garden," rapidly became a ghetto, then a ghost town, as subscribers deserted it for more innovative and open service providers that came online. Apple fared better because of its quality software, but found that its pursuit of a broad consumer market for its phones and tablets forced it to become more open to apps from anyone. However, as Internet researchers, such as the OpenNet Initiative, have taught us many states have also enclosed the cultural commons for their own benefit—many are building "walled gardens," where their citizens can access only their version of the truth and other information that does not contradict it.[3] This is accomplished technologically by blocking access to suspect foreign sites, blocking search engines from returning pointers to information on "forbidden issues," cancelling service for politically unreliable sites and blogs, subjecting them to denial-of-service attacks, etc. Unlike in the AOL and Apple cases, those who would leave the walled garden through some "jailbreak" risk jail or worse. State authorities can likely identify them through surveillance technologies, in some instances, sadly enough, purchased from companies that got their start on the open Internet.

These assaults on the Internet are not confined to destroying the cultural commons. They also disrupt social media, where state security agents masquerade as anti-government activists, and attack the Internet's trust layer. In a notorious incident, Iranian hackers secured fraudulent certificates from a Dutch certificate authority, apparently so state security agencies could "authenticate" bogus versions of sites that Iranian (or perhaps Syrian) activists would visit (having been directed to them by poisoned DNS).[4]

Yet, just as the Internet affords Iranian hackers and their handlers opportunities to become high-tech versions of the traditional agent provocateur, so it updates the traditional role of the free speech advocate, the printer of forbidden books, or smuggler of clandestine texts. Whether through legal fights, technology development, hacking, or documenting filtering, those who enable the flow of packets around barriers erected to protect copyright or regimes present one definition for "cyber steward." This role is not particularly heroic, though it has sometimes earned crippling retaliations from law enforcement and state security agencies, and playing it is not always justified. As already noted, Lessig concedes some legitimacy to copyright enforcement, and many free speech advocates admit some limits, for example, child pornography, Nazi memorabilia, or "falsely shouting fire in a crowded theatre" – the question not being whether there should be limits, but where the limits are and how are they decided.[5]

The motivations for this type of stewardship are varied. Some people active in circumventing the

3 Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, MA: MIT Press, 2008); Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010).

4 Toby Sterling, "Iran Involvement Suspected in DigiNotar Security Firm Hacking: Experts," *Huffington Post*, 5 September 2011, http://www.huffingtonpost.com/2011/09/05/iran-diginotar-hack_n_949517.html.

5 US Supreme Court Justice Holmes later regretted his application of the "fire in a crowded theatre" (creating a clear and present danger) test to Schenck v. Ohio which upheld the conviction of Socialist party leaders for violation of the 1917 Espionage Act by distribution of anti-draft literature.

media crackdowns in recent Middle East protests are committed to specific groups of protesters. They are expatriates or exiles who used technical skills and rapidly acquired understandings of media campaigns to turn cyberspace into a battleground and, more importantly, organizing tools. Their concern for openness is not to protect a cultural commons or public sphere, as much as to exploit cyberspace for their political struggles—a valid goal, under the circumstances, but a narrower one. In contrast, some activists and researchers bring to their "cyber stewardship" an involvement in the struggle against censorship, often out of a commitment to human rights, defined as including rights to information and expression. Their facilitating the cyber dimensions of particular political actions is thus an instance of a lengthier, broader struggle, with motivations not bred in cyberspace, but focused on it because it is now the main battle theatre. (In this respect, they have counterparts in anarchist initiatives, like Wikileaks, Anonymous, and Lulzsec, which find in cyberspace the means and opportunities of satisfying an older dream of discrediting governments and the powerful by exposing their secrets.) Among people with commitments more specific to an open Internet are the "geeks" who, Christopher Kelty saw, constitute recursive publics. That is, they imagine themselves a group associated through the means of the Internet and spend considerable time discussing, building, and rebuilding this means of association. Kelty's characterization of geeks' discourse captures their fervid notions of "cyber stewardship" and the "cyber commons"—both matters of their own survival as a group.

When geeks argue, they argue about rights and reasons, but they also argue about the Internet as the technical structure and legal rules that allow them to argue in the first place. Furthermore, not only do they argue about these structures and rules, but they consider sacred the right to change these rules by rewriting and reimplementing the core protocols (the "rules") and core software that give the Internet its structure; they also consider it essential that individuals and groups in society have the right to reimplement privately ordered legal regimes to achieve these ends. These arguments are neither idle nor do they represent how the Internet "really is"—they are imaginaries of what gives the Internet its present order or how it should be ordered in the future.[6]

Many shared libertarian and antinomian values are encapsulated in the slogan "information wants to be free," attributed to Stewart Brand,[7] and in John Gilmore's claim that "the Net interprets censorship as damage and routes around it" that is, we learn to route around censorship. Such values are also inherent in the name of the Internet rights advocacy group, the Electronic Frontier Foundation (EFF).

The United States has financially, rhetorically, technologically, and selectively supported "cyber stewardship" as part of its foreign policy. In its policy-makers' views, this aid helps the US gain influence, increase its cultural attraction, bolster Internet freedom for its own sake, and in some cases, promote regime change at a low cost. Such aid may have unwittingly contributed to Mubarak's downfall, but the US has not reproached its allies Saudi Arabia and Bahrain for their very restrictive Internet policies. The policy can also clash with other American efforts to shape the cyber commons. While the US State

6 Christopher Kelty, "Geeks, Social Imaginaries, and Recursive Publics, *Cultural Anthropology*, 20, no. 2 (2005): 186.

7 By happy coincidence for this essay, that is the name of the 1970s onward counter-culture guru. What Brand said approximated the slogan but it was part of his speaking about the tension between information's distribution costs tending to zero, thanks to the cyber networks, and its high production costs.

Department criticized China's blocking access to sites, the US Congress considered legislation that would require American service providers to do the same to foreign sites alleged to serve pirated movies and music. The targets of this sponsored stewardship can thus easily accuse the US of hypocrisy in promoting cyber rights. In their view, the US wants to weaken regimes in order to retain its dominance in world affairs, and it wants to weaken a regime's control of its territorial cyberspace to prolong American domination of the Internet. The "cyber stewards" are consequently dupes or, more charitably, partners in a marriage of convenience.

TAKE 2: THE COMMON CYBER STEWARD

The EFF's foundational image is the American frontier of the eighteenth and nineteenth centuries, where supposedly "if you saw the smoke from your neighbour's chimney, it was time to move on." Yet such individualism and independence might be inappropriate for cyberspace. When it was still a place rather than multitudes of computational routines woven into the fabric of life worlds, many of us were online because others were, and they were online because we were. By the late 1990s, digital communities (of interest) were pervasive. As checking in with one's communities went from occasional to continual, with apps and devices supporting that change, digital communities flattened into today's social media—but the idea of community persists. Being in a community, even a virtual one, creates rights and duties to others, because, even at a minimum, your actions can affect others and theirs can affect you, regardless of intention.

The notion of online duties is particularly apt when the community, its members individually, and its cyber basis are under attack from a variety of cybercrimes, botnet enslavement, surveillance, privacy-denying tracking, gratuitous malware, etc. One response to these threats, the computer hygiene approach, turns the common user into a line of defence, a "cyber steward," as it were, charging her with the imperative: "don't get sick, and, if you do, don't infect others." Viruses and contagion, as the terms imply, are readily seen as disease-like natural phenomena. The user, in theory, is expected to handle their prevention and remediation, armed with anti-virus software, spam filters, vigilance for phishing, up-to-date patches, and some clues about the technologies at the host and network level that lie behind the screens. However not everyone who accesses the Internet is that security conscious, and, as the hacking of RSA security shows, even folks at cybersecurity firms can succumb to social engineering or other sophisticated attacks. So typically the user delegates the responsibility for prevention, relying on her ISP or organization to deal with the vulnerabilities, which the hardware manufacturers, software developers, network architects, and the user herself create. Delegation transforms the hygiene into a public health issue, but it also invites moral hazards, if the service provider or other agent tasked with prevention lacks the incentive or capability to handle it. One solution to that problem is regulation, which parses the risks or vulnerabilities according to parties who created them and who has the capabilities to fix them; then it assesses the liability of parties that fail to fix their vulnerabilities.[8] In political-economic terms, regulation would make members of the community suppress or absorb their own negative externalities.

8 My thanks to John Mallery for this understanding of cyber regulations. Of course, almost all of these parties oppose the imposition of any regulations.

The public health approach can also involve defensive coordination across end users at various levels, through agents like industrial sector information sharing and analysis centres (ISAC), regional public-private partnerships, national CERTS, and international alliances of CERTs. The recent United Nations General Assembly resolution for the "creation of a global culture of cybersecurity" gently suggests that a national program would include industry, academia, and civil society and should train individual citizens to avoid online threats.[9] The model is vulnerability driven and non-agonistic in contrast to threat-driven models, which aim to suppress the sources of threats but are bedeviled by problems of attribution and multiple jurisdictions. Yet, this stewardship will have expectable limitations, even in the best case of enforced, insightful regulations and effective coordination among stewards. The vulnerabilities of rapidly developing cyber technologies, applications, and use will likely exceed the resources of prevention and defence agents. The rapid growth of Internet-connected devices and users has greatly expanded the attack surface and brought online many technologically less-sophisticated users who access through more vulnerable systems, such as wireless. Depending on its type, an attack might need only one point of access to considerably damage a network. Meanwhile the sophistication of the threats has increased, so one can fear, as Stanley Baldwin did about the growth of airpower in the 1930s, that "the bomber will always get through," and agree the "only defense is in offense."[10]

TAKE 3: THE STATE AS CYBER STEWARD

In the public-health model the various prevention agents derive authority from acting on their own behalf or having responsibility delegated to them by entities that ideally could act on their own. In the state-centric model, the state agencies claim their authority to control a national cyberspace as part of caring for the society as a whole. Such a claim is evident in the recent Chinese white paper, which celebrates the Internet for enabling economic and social development and notes its use in propagandizing the public and in campaigns against provincial corruption, but cautions that

> "no organization or individual may produce, duplicate, announce or disseminate information [on the Internet] having the following contents: being against the cardinal principles set forth in the Constitution; endangering state security, divulging state secrets, subverting state power and jeopardizing national unification; damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations".[11]

Arguably such restrictions descend from China's Marxist-Leninist heritage, in which the party and its state enforcer are the vanguard of the people making the needed decisions for them. That notion in turn came from Rousseau's "general will" or the true interest of the society, as opposed to the aggregation of individual interests. Accordingly, leadership, which organizes

9 United Nations, A/res/64/211. http://www.citizenlab.org/cybernorms/ares64211.pdf

10 Brett Holman, "The Bomber Will Always Get Through," Airminded: Air Power and British Society, 1908-1941, Blog, 10 November 2007, http://airminded.org/2007/11/10/the-bomber-will-always-get-through/.

11 Information Office of the State Council of the People's Republic of China, "The Internet in China," 8 June 2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm.

society for the general will, needs to maintain control of the ideational space. The diversity of ideas and interests presented by the Internet is consequently a threat to both the leaders and the society – a form of information warfare. Of course, whatever their ideological lineages, authoritarian governments as a rule will attempt to suppress dissent, often with a similar self-serving claim of acting to preserve social harmony.

However, in many countries, even in liberal democracies, various state agencies have sought some control of their "national cyberspaces", on the grounds of national security. By the late 1990s, signal intelligence agents in states as different as the United States and Russia were tracking Internet users out of concern that terrorists were using the Internet for propaganda, recruitment, fundraising, and coordination. Following 9/11, the US Congress expanded authorization of such activities in the US, although it stopped short of permitting the "total information awareness" that some security agencies sought. The cyber-network attacks on Estonia in 2007, then Georgia in 2008, along with news of Stuxnet alerted technologically developed nations to the vulnerability of both their critical infrastructures and the digital networks used by their military and security organizations. In addition, the theft of American intellectual property in cyber exploits originating in China has been so persistent and extensive that the US government now considers it another threat to national security. Various responses to these threats have included setting up a military command dedicated to cyber defence and offence, integration of cyber defence in NATO's new strategic doctrine, assigning some role to the military in protecting cyber-dependent civilian infrastructures, and proposals to extend the state-centric international system into cyberspace.[12]

These efforts at securing cyberspace — "stewardship" in a way — are not driven by a need for ideological hegemony, but they can still endanger the cyber commons, especially with respect to its openness to innovation and global conversations. First, with national security at issue, states are more likely to favour centralization of information systems, monopoly, and national champions, at the expense of innovation.[13] Second, implementing national boundaries in cyberspace, say, by aligning local DNS root servers with blocs of IP addresses issued to countries, will embed a principle of national sovereignty in the Internet's protocols. That would encourage fragmentation – the oxymoron of an "Internet in one country" – and facilitate censorship at the operational level, while sacrificing the grounds for criticizing such developments.

The principle of national sovereignty as articulated in the Treaty of Westphalia, the foundational document of our international system, gives a ruler or state the right to manage the minds of its subjects: "Cuius regio, eius religio." In return, the state supposedly accepts responsibility for any attack originating in its territory against another state and acts to prevent its subjects from interfering in another state's internal affairs, including the control of its subjects' minds. The United States can therefore demand that China suppress the industrial espionage that originates from China. By the same token, however, the Chinese government can complain that the United States fails its sovereign responsibility in permitting Chinese dissidents in the United States to serve "disruptive" material to Chinese citizens. Indeed, the Shanghai Cooperation Organization's Agreement on Information Security and the recent Russian proposal for international cyber norms give the targeted state the right to determine

12 Chris Demchak and PeterDombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, 5, no. 1 (2011): 32-61.

13 Tim Wu, *The Master Switch* (New York: Knopf, 2010).

which information threatens it.[14]

State-centric stewardship takes a very pragmatic approach to the digital networks and routines that constitute cyberspace. They are means for organizing social, economic, and cultural life within the society and for projecting hard and soft power. They need to be protected from attacks, which could impair their fulfilling these functions. This apparent subjection of cyberspace to national interests calls into question the utopian notion that cyberspace will nurture a global consciousness – a meeting of minds from all over the world. Westphalia's principle of national sovereignty may have provided the best solution for the seventeenth century's deadly wars of religion, but applied to cyberspace, it threatens the development of a platform for bottom-up discussions of global issues. The claim that it is needed to protect cyberspace recalls the sad joke of having to destroy the village in order to liberate it.

TAKE 4: TRUST

Taking a somber look in 2010 at the growing crisis of cybersecurity, a United Nations group of experts recommended "dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure."[15] This prompted some buzz about the possibilities of an international cyber treaty that would provide internationally accepted definitions of illegal and hostile acts in cyberspace and possibly prompt signatories to the treaty to prevent them.[16] The prospects for that happening, however, are slight, despite many governments and organizations recognizing that benefits provided by the Internet might be a risk and that conflicts that begin between states in cyberspace could escalate into kinetic violence.

There are multiple reasons for this pessimism. First, the billions of devices, their increasing mobility, and the problems of attack attribution raise the cost of policing any agreements, while limiting its scope and efficacy. Second, for the present, cyber usage, economies, and cultures continue to grow spectacularly. Even if the insecurities diminish public trust, the consequences will not be felt for a long time, so there is little pressure for governments and other stakeholders to act now. Third, notwithstanding their agreement on the need to discuss norms, cyber powers like the US, Russia, and China disagree on what those norms should be. As we have seen, they differ deeply over information rights, protected speech, and the separation of content from carriage, but also over norms for intellectual property rights and governance. China, other SCO members, and many of the former "non-aligned" nations believe that the state should be the final arbiter of cyber matters within its territory. They would like the Internet administered by the ITU or a new UN agency in which each state has one vote. The US and its allies favour a multistakeholder model, where corporations and technologists, many of them American, join states in making policy, and the US champions

14 "Convention on International Information Security," presented to the Second International Meeting of High-Level Officials Responsible for Security Matters, Ekaterinburg, Russia, September 2011. For a discussion of states' defining dissident information as a security threat and of hosting dissidents being defined as rising to information warfare, see Tom Gjelten, "Seeing the Internet as an 'Information Weapon,'" NPR, 23 September 2010, http://www.npr.org/templates/story/story.php?storyId=130052701.

15 UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201, 30 July 2010, http://www.unidir.org/pdf/activites/pdf5-act483.pdf.

16 There is some evidence that the one major cyber treaty, the Budapest Convention on Cybercrime has produced some reduction of cyber attacks coming from its signatory countries. See Seung Hyun Kim, Qiu-Hong Wang, and Johannes Ullrich, "A Comparative Study of Cyberattacks," *Communications of the ACM*, 55, no. 3 (March 2012): 66-73.

ICANN to administer the Internet.

Beyond these specific differences, many states distrust the US on cyber matters because of the Internet's association with American triumphalism of the 1990s. It emerged as the US declared victory in the Cold War and that history, that is, class struggle, had ended in the triumph of liberal capitalism. The Internet was enabled by the liberalization of the US telecommunications sector, a policy model for other states, and the Internet in turn has supported the spread of NGOs and civic activism in former Soviet satellites. Although the Internet's killer app, the World Wide Web, was created in Europe, it was rapidly remade in the US with American-designed browsers. Using this application, American start-ups like Yahoo, Amazon, and Ebay started organizing worldwide businesses. In short, the Internet was a vehicle for American soft power: the combination of technology, business, politics, and culture it projected appeared to be mandatory for online success. But this may no longer be the case. China and other countries have achieved significant usage, online economies, and social media despite political repression. Now with the US accounting for only 10 percent of users, the "made in the USA" label on the Internet can look very dated. Many states, consequently, question the superiority of the old model and believe the US's insistence on it is a ploy to retain control of the Internet to facilitate sales of American technology that supports it.

Amid such distrust, states and other organizations can become useful "cyber stewards" by initiating confidence-building measures, which in turn might improve conditions for reaching effective treaties. Although symbolic, high-profile measures such as a hot line are frequently mentioned—initiatives that are closer to the daily operational levels will more likely gain traction. A prime candidate for such an initiative is the development of local cybersecurity capabilities, whose importance is already recognized by both the UN resolution on creating a global culture of cybersecurity and the United States' international strategy for cyberspace.[17] Successful cooperation among countries with high capabilities in training personnel elsewhere can decrease the number of countries in which the launch of international cyber attacks evades the attention of local officials. It would also diminish the suspicions that now arise when such officials claim they cannot stop the attackers, and it could provide career opportunities for officials who do want to protect cyberspace. Similarly, working alliances among national CERTs and informal collaborations of national police in cyber investigations can accustom upper-level officials to seek common ground on cyber issues, notwithstanding cultural and political differences. Thus, China's Minister of Public Security said, after an unprecedented operation involving his police and the FBI closed down a child pornography ring: "Although China and the US have different judicial systems and cultural values, the two sides share a common view in crime-fighting." The Minister then pledged that China would continue to strengthen its law-enforcement cooperation with foreign countries and vigorously fight transnational illegal activities, especially crimes committed through the Internet.[18] Existing business relations can also be leveraged for confidence-building measures. In particular, some certification of ICT hardware and software supply chains are needed to dispel distrust about the integrity of chips, components, or programs

17 "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," White House, Washington DC, May 2011.

18 "Chinese Police Chief Vows International Cooperation in Fighting Internet Crimes," *Xinhua*, 30 August 2011, http://news.xinhuanet.com/english2010/china/2011-08/30/c_131085036.htm.

and the absence of Trojans, backdoors, etc. Certification would be in the interests of both suppliers and consumers, since doubts are reportedly leading some governments to insist on the more costly path of having components in military and critical infrastructure systems being built on their national soil. It would, however, require participation of companies as well as governments.

International confidence regarding cyberspace would also benefit from some discussion of whether and what cyber attacks might be defined as "armed attacks" and so amount to an act of war. As noted before, ambiguities regarding this matter have fed anxieties about unintended cyber conflicts and their unwanted escalation. Because nations have not and probably will not unilaterally specify their redlines, there is considerable opportunity for miscalculations and misperceptions. For example, a state might launch what it considers an "acceptable" cyber operation, like probing another state's cyber defences, but the target state considers the operation hostile and would retaliate, if it could positively identify the perpetrator. The history of interstate engagements over cyberspace provides little guidance for dealing with such ambiguities or for a discussion among states that would define a "cyber armed attack." Some items in that history, however, suggest a bias against considering cyber attacks "acts of war" or justifications for widening a conflict.

- In the few cases where a cyber operation was generally considered a "hostile act" and a particular state actor believed to have been responsible for it, the state actor denied responsibility or remained silent, while the targeted state did not retaliate or press a case against the suspected perpetrator.[19]
- In 2011, NATO rejected a recommendation that its new strategic doctrine specify that any cyber attack on a member state would trigger consultations (Article 4) and some attacks could trigger an armed response (Article 5). The recommendation sought to regularize responses to events like the 2007 DDoS attacks on Estonia, a NATO member, which had left the alliance fumbling for a response. The NATO decision makers instead preferred the freedom to decide the alliance's response on a case-by-case basis.
- Government officials have generally avoided branding a cyber action as a "hostile act," much less an "armed attack", and have also avoided attributing exploits and attacks to particular governments. Thus, US Chief of Staff Richard Dempsey told a Senate hearing that he could not attribute the large-scale espionage originating in China to the Chinese military and that he would characterize it as a crime, rather than a hostile act.[20]

Such restraint might be due to the relatively low capabilities of currently deployable cyber weapons and the untested effectiveness of more potent weapons under development. Hopefully, it might also involve a stewardship or concern among national security officials to keep cyberspace from turning into a battlefield.

19 Estonia (2007) was attacked by Russian hacktivists; Georgia (2008) was attacked by Russian hacktivists, likely coordinated by Russian government or military; Syria (2007) missile defense defence was reportedly neutralized through cyber means by Israel as part of Israel's destruction on an alleged nuclear reactor in Syria; in Iran (2010), the Stuxnet worm, allegedly developed by US and/ or Israel, was used to destroy centrifuges in the Iranian nuclear development program.

20 Adam Levine, "Joint Chiefs Chair: Chinese Hacking Not Necessarily a Hostile Act," CNN, 14 February 14 2012. http://articles.cnn.com/2012-02-14/us/us_dempsey-china-hacking_1_joint-chiefs-dempsey-top-military-officer?_s=PM:US.

OUTTAKE

There is a utopian element in the notion of cyberspace. It is a vision of a technology that is built on openness—that nurtures innovation and provides a platform for a global culture. Some of that vision has been realized, some has not. As noted, some cyber stewards are driven to pursue those missing parts as the keys to ever more freedom. Perhaps that is overreaching in view of the growing threats to what we already have. Just before his recent death, historian Tony Judt speculated that "we are at the end of a very long cycle of improvement," that began in the late eighteenth century, continued until a few decades ago, and was associated with the spread of individual freedom and rule of law.[21] He suggested that because of the threats to this cycle, most notably growing economic insecurity, the way "to defend and advance large abstractions in the generations to come will be to defend and protect institutions, laws, rules and practices that incarnate our best attempt at [realizing] these large abstractions."[22] This call to vigilance and defence sounds like marching orders for cyber stewards.

Roger Hurwitz is a Research Scientist at MIT's Computer Science and AI Lab (CSAIL), a senior Fellow at the Canada Centre for Global Security Studies at the University of Toronto, and a founder of Explorations in Cyber International Relations (ECIR) at Harvard and MIT. A Ph.D. in computational social sciences, his research and writing include modelling conflict escalation and de-escalation, Middle East politics, measuring information flows, content analysis and hermeneutics. He has taught at MIT, Northeastern and the Hebrew University, and co-developed (with John Mallery) the White House Electronics Publication System and the Open Meeting platform for wide-area online collaboration. His current work includes the development of a computational system for cyber events data and ontologies, and modelling the complexities of cyber incidents.

Research for this paper was partly funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research

21 Tony Judt, "On Intellectuals and Democracy," *New York Review of Books*, 69, no. 5 (22 March 2012): 7.

22 Ibid.