The New Atlantis
A Journal of Technology & Society

The Trouble with Cyber Arms Control

Christopher A. Ford

These are early days in the age of cyberwar. In the developed world, nearly every sphere of life now depends upon computers and networks, a fact that has introduced great vulnerabilities. The United States in particular—with a modern infrastructure, a plugged-in population, numerous enemies and competitors around the world, and a military whose overawing conventional prowess is heavily reliant on computer networks—has reason to feel exposed to cyber attack.

U.S. Department of Defense computer systems are already probed millions of times a day by would-be computer intruders. Some succeed in becoming more than would-be intruders, such as the still-unidentified assailants who not long ago managed to access terabytes of files related to the new F-35 Joint Strike Fighter jet. Computer espionage is already an established tool of twenty-first century geopolitics, and attacks upon computer systems and networks are now emerging as a powerful tool of warfare. When Russia invaded the Republic of Georgia in 2008, Georgian computer systems were subjected to crippling attacks intriguingly coincident with the sudden Russian offensive—an event some consider to be the first wave in the new tide of cyberwar. Palestinian and Israeli hackers reportedly attacked each other's computer systems during the Gaza conflict in 2008-09. And more recently, the Stuxnet computer worm seems to have damaged work on Iran's nuclear reactor at Bushehr and the country's ongoing uranium enrichment operations at Natanz. Computer attackers—whether they be hacker-activists aligned with no government, cyber privateers quietly encouraged by a government, or authorized governmental cyber soldiers—seem likely to play increasingly important roles in future conflicts.

In light of this new trend in warfare and what is presumed to be our enormous vulnerability to its techniques, it is no surprise to hear calls for what amounts to cyber arms control. Indeed, such is our collective reflex for addressing novel threats by attempting grand exercises in treaty-making that it would be shocking if the advent of this new and highly

***Christopher A. Ford**, a* New Atlantis *contributing editor, is a senior fellow at the Hudson Institute. His book* The Mind of Empire: China's History and Modern Foreign Relations *was published in 2010 by the University Press of Kentucky. He blogs at NewParadigmsForum.com.*

disruptive military technology—one so well-suited to wreaking havoc upon a civilian economy—were *not* soon followed by calls to try to bring it under the control of some sort of cyber weapons convention. Russian and other diplomats have already started to make noises to this effect, and when asked in June 2010 about Russia's suggestions, General Keith B. Alexander, the head of United States Cyber Command, indicated potential interest in exploring the idea.

Cyber Arms Control: Look Before You Leap

But we should be careful what we wish for. It may be that some sort of arms control agreement can indeed contribute to reining in the cyber threats we face. When evaluating such proposals, however, we should be careful not to let our judgment run away with our principled enthusiasm for a congenially treaty-based diplomatic "fix." As always, the devil may lurk in the details, and arms control is too important, too potentially valuable, and too potentially dangerous to be done badly.

A first concern is that any attempt to ban cyber "weapons" seems all but certain to run afoul of verification problems that would make those of the Biological and Toxin Weapons Convention seem simple by comparison. It has proven impossible to negotiate a verification protocol under that treaty precisely because dual-use biotechnology capabilities are so widespread and easy to conceal that even the most intrusive and disruptive monitoring procedures would be inadequate to the task. One can only imagine the additional complexity and difficulty when the "weapon" in question is not even physical. However, there might conceivably be some symbolic value in a ban on certain particularly indiscriminate or mass-disruptive techniques or effects in order to establish a norm against them. There might also be practical value in some kind of agreement on transnational cooperation in cyber forensics, to aid in determining who perpetrated attacks.

But it is crucial to understand that, as we do with proposals to reduce threats to our essential and highly vulnerable space-based communications and sensor systems, we should carefully scrutinize arms control proposals made by those who do not necessarily share our interest in addressing the potential threat presented by cyber attacks upon the developed world's sprawling computer and communications systems, or by those who may have additional and less salutary goals in mind. Even when proposals for treaties are presented in ways that appeal to our sense of what an international legal remedy should look like—and indeed, perhaps *especially*

then—we must be alive to the possibility that what seem to be solutions may in fact be intended by others to bring about very different ends than we might desire.

A prime example of this point is the proposal for a treaty for the Prevention of an Arms Race in Outer Space (PAROS). The treaty has been advocated for years by Russian and Chinese diplomats in the Conference on Disarmament in Geneva, and the United States has since the days of Jimmy Carter consistently refused to enter into discussions about it, although the Obama administration has now reversed this stance. It is unquestionably true that an anti-satellite war would disproportionately degrade U.S. military capabilities, especially the ability to project global power. But that threat does not necessarily mean that it is in our interest to accept these or other prominent proposals for a space arms control treaty. There may be value in developing agreements on space-related "best practices," perhaps of the sort presently being negotiated under European Union auspices—a sort of code of conduct for activities related to space. But not all proposals for space arms control are being made in good faith, and not all of them would, at least from a U.S. perspective, actually improve the situation.

Most notably, the PAROS proposals that have long been promoted by Russia and China—which have garnered a remarkable amount of support from other governments that should know better—are actually designed to facilitate the Russian and Chinese capacities to deny the United States access to needed space assets, including limiting our options for ballistic missile defense. Both Moscow and Beijing have operational ground-based anti-satellite weapons (ASATs), with the Russians having possessed such weapons for decades and the Chinese having demonstrated their own in 2007. The United States also has a *de facto* ASAT capability in its current anti-ballistic missile weaponry, which we demonstrated in 2008 by destroying an errant U.S. spy satellite before it could cause harm in crashing to Earth. But our potential adversaries are less dependent upon space assets than we are. This makes ASATs a classically "asymmetric" capability, disproportionately useful against the American hyperpower. It is no secret, then, why planners in Moscow and Beijing are so interested in ASATs, and why we worry about their potential capabilities.

From the perspective of arms control enthusiasts, our vulnerability to attacks in space underlines the importance of space arms control. If we are disproportionately vulnerable, after all, why not try to limit or ban space-based weapons? This analysis is not wrong, as far as it goes. But it is not at all clear that an agreement could be crafted that would actually help.

Indeed, it could be argued that the Russian and Chinese PAROS proposals themselves represent tools of asymmetric conflict, because their ban on weapons "in outer space" would pointedly leave unregulated the *ground*-based ASAT systems Russia and China possess—all while prohibiting any potential future deployment of an American capability those countries do not wish us to have: space-based defenses against ballistic missiles. Nor is it clear that an alternative effort to control or prohibit all anti-satellite technologies would be feasible, enforceable, or even desirable.

The PAROS example illustrates the need to critically examine proposals to export traditional arms control approaches into new arenas. It may indeed be possible to help reduce threats by bringing arms control into outer space—or into cyberspace. But, especially given the eagerness of other parties to co-opt such proposals to serve their own ends, we would be wise not to accept them uncritically.

What is Cyberwar?

Before we consider international proposals aimed at curbing cyber threats, it is crucial that we first understand what each of their advocates judges the threats to be. When Americans speak of cyberwar, we tend to think of lines of malicious code being sent from one computer to another, generally via the Internet, in order to cause some kind of mischief: say, taking down a power grid, or crashing the control systems for an air-defense network. But in fact, the line between computer-on-computer attack and other forms of electronic assault is quite fuzzy, and future cyber conflicts between sophisticated players may see wildly different means and ends that we cannot now predict.

While acknowledging these ambiguities, however, it is worth noting that we almost always conceptualize cyber attack in *technical* terms—in terms of the tools and methods used in an attack, or their targets. To U.S. strategists, cyberwar strategy usually means protecting our computer and communications systems against disruption or degradation from hostile computers, while retaining the ability to inflict such disruption upon a potential adversary. The analogy to physical weapons—that is, military tools that actually smash or explode things—is in this conception quite close: cyber "attack" is about destroying or degrading the operation or effectiveness of adversary systems, objects, or infrastructure.

An alternative way of discussing cyberwar is in terms not of technology but of *influence*. In U.S. military doctrine, "information warfare" or "information operations" (IO) are somewhat separate from cyber conflict.

Information operations in time of conflict include psychological operations, such as deception and perception management; familiar examples from the twentieth century include dropping leaflets from airplanes, running strategic misdirection operations, and broadcasting propaganda. Recently, this category has broadened to include even such activities as giving interviews to the press or writing opinion pieces for newspaper publication, as well as protection and assurance activities directed at preserving the integrity and availability of one's *own* information. In the American understanding of the terms, therefore, not all IO is cyber in nature, but the two can overlap: cyber attacks can be used as a tool for accomplishing IO goals. For example, a combatant might hack into an adversary's systems to plant false data or stories intended to sow fear or confusion. Still, cyberwar and IO are not synonymous, and the former is generally conceived by U.S. analysts in more narrowly technical terms. As we shall see, however, this distinction is not universally shared; Russian and Chinese military doctrines blur the concepts considerably.

In this regard, it is also worth paying close attention to the word "cyber*war*" itself: we tend to conceive of cyber conflict in terms of *warfare*, as a matter of attack and defense. Some critics, such as respected security expert Bruce Schneier, have cautioned that overuse of the term "cyberwar" can unduly inflate the risks we are facing and may warp our priorities. But inasmuch as a cyber attack is a discrete and deliberate act of harm that is in some sense "launched" by one party against another, the Western strategic approach has tended to regard it as roughly analogous to a conventional military attack. As discrete, deliberate, and concrete acts of hostility, cyber assaults are assumed to occur within a paradigm of warfare between combatant adversaries, even if the harm they impose does not always directly result in physical destruction or casualties. And our military planners assume that at least *our* use of cyber weapons, like all weapons, should be governed by the traditions embodied in the law of armed conflict—including the concepts of military necessity, proportionality, and discrimination (or distinction) between combatants and noncombatants.

Proceeding from this starting point, it is easy to conceptualize the problem in terms of some form of arms control in cyberspace—at least in principle. Making it work may be tricky in practice, but it is perhaps not so demanding in theory. One would have to get past the challenges of trying to define the things that are to be controlled, and of verifying and enforcing compliance—all of which might well prove intractable when the "weapon" at issue is as intangible as computer code—but aside

from this, there might seem to be nothing inherently problematic about the notion of cyber arms control. In the traditional model of arms control, after all, one identifies the type of weapon or behavior that threatens peace, and then simply proscribes it.

But practical *and* theoretical concerns about cyber arms control—and thus its inherent desirability—may be much more problematic if one defines the threat from an alternate conceptual framework. Judging by what little is presently known or believed about Russian and Chinese notions of cyber conflict, Moscow and Beijing seem to have a very different idea than we do about the problem that is to be solved by "arms control." To the extent that they might differ from us in our understanding of cyber attacks as essentially similar to conventional military attacks, we should be especially wary of their proposals. While all developed nations surely share a powerful interest in preventing massive network-borne disruptions caused by malicious code, some governments have broader ideas than others of what constitutes a cyber threat—to the point that some consider it threatening for their citizenry just to have uncensored access to the World Wide Web. This disparity means, to put it crudely, that some arms control proposals may turn out to be designed to address "problems" that it is quite contrary to our interests to "solve."

The Russian Conception

There is little official information available on Russian cyberwar doctrine. Nevertheless, some unclassified writings by Russian strategists are available, and have been pored over by Western experts. Rather than stressing the offense and defense of computer systems, Russian doctrine emphasizes the importance of information operations—of psychologically distorting a target's model of the world, thus influencing his behavior. Far less attention has been devoted to the tools actually used. Prominent Russian analysts seem to believe that an "information weapon" can be almost *anything* that has the desired impact on the targeted minds. (Note that *minds* are viewed as the target, rather than electronic or physical *systems*.) In the words of one, "any technical, biological, or social means or system" could count.

As observed by Timothy L. Thomas, an American expert on Russian and Chinese cyber and information warfare strategies, Russian thinkers tend to break IO issues into specifically "information-technical" and "information-psychological" components. The "information-technical" component essentially overlaps with the American conception of cyber-

war. "Information-psychological" conflict, however, brings in a broad Russian understanding of the potential usefulness of the Internet and mass media in affecting the beliefs and attitudes of the adversary—not just its military or senior political leaders, but indeed its civilian population as a whole.

The cognitive aspects of Russian IO are thus at least as important as the technical ones, and probably more so. Russian thinkers have developed theories of what they call "reflexive control," in which information is manipulated in order to elicit favorable actions by the adversary. This manipulation is meant not just to occur at the level of wartime expedience, against the computer systems involved in data-driven decision-making by enemy leaders, but also as a tool of strategy and politics in the grandest sense. Its goal is to exert influence over the adversary's politics, both internally and in its relations with other states. Russia thus appears to possess a totalistic ideal of information warfare as a contest between *whole societies*, waged by all available means across a broad spectrum of information "fronts." In this conception, the Internet is not merely the medium through which cyber-warriors reach target computers and other electronic systems, but more generally the means for waging "information-psychological" combat to influence the minds of mass audiences. In fact, information attacks seem to be considered more useful in times of peace than in times of war. In peacetime, according to Russian writers, IO activity should include such steps to protect the state as thwarting possible adversary coalitions and attempting to shape public opinion—both that of the Russian people and that of the civilian populations of adversary countries.

These conceptions clearly reflect continuity with Communist-era understandings of propaganda warfare. Soviet doctrine on so-called "active measures" and "disinformation"—notions that would fit under today's broad conceptions of IO—was quite well developed. The Soviets were also early pioneers of cyber techniques: they reportedly began to investigate computer intrusion in the mid-1970s, and in the 1980s the KGB hired a German hacker to try to steal information on ballistic missile defenses from U.S. computers. But Soviet concepts of "active measures" were based upon a much broader idea of how "information" could be used as a tool of national strategy. As befits an authoritarian system organized around a totalizing ideology, the Soviet Union did not sharply distinguish between action and propaganda; its theory of "active measures" stressed the employment of broad strategies to influence the politics of other governments, undermine confidence in their leaders and institutions, disrupt

relations between otherwise-friendly states, and discredit and weaken major opponents by deceiving target audiences and distorting their perceptions of reality.

This continuity between Soviet and post-Soviet Russia is revealing. It shows us, first, that the Russian doctrine toward cyberspace applications of information operations is not just about what Moscow may do in *offensive* situations. But it also tells us a great deal about what Russia fears—and therefore, presumably, about what might motivate the Kremlin's understanding of cyber arms control.

As Thomas has recounted, Russian military theorists have always been concerned with the potential influence of their adversaries upon the morale and psyche of Russian soldiers. The "moral-psychological" preparation of the soldier is consequently seen as critical to Russia's success in war. From the Bolshevik Revolution through Stalin's brutal reign to the present day, from the rise of the sprawling Soviet empire to even after its dissolution into a kaleidoscope of fissiparous republics, Russian strategic thinkers have firmly held on to the notion that information, in the form of *thought*, could imperil the security of the state. In the 1990s, perhaps influenced by conspiracy theories that the collapse of the U.S.S.R. was instigated by subtle Western psychological operations, Russian thinkers came to see their society as highly vulnerable to disruptive outside influences. Writings during this period, as Thomas has described, emphasized the need to counter "information expansionism" by Russia's adversaries. National security was seen as requiring increased efforts to ensure what one Russian author called the "functional reliability of the psyche and consciousness of a person in peacetime or wartime" with respect to Russian society as a whole. Thus viewed, the rebirth of Russia as a power on the world stage was inextricably bound up with the dynamics of "information-psychological confrontation."

Not surprisingly given this view, Russian approaches to information warfare and its cyberspace applications have placed considerable emphasis on controlling the content of mass media, with an eye toward shaping both foreign and domestic perceptions. Numerous Russian studies refer to the problems of inadequate control of this sort, which they claim is apparent in the Soviet war in Afghanistan, in the first Chechen war of 1994-1996, and in Moscow's handling in 2000 of the *Kursk* submarine disaster. These studies suggest, however, that the state more adroitly handled the information aspects of the second Chechen war (1999-2009). In this second phase of the conflict, Russian officials used both state-controlled media and semi-official websites to disseminate their perspectives, pressed

journalists to follow Russian guidelines for covering events in Chechnya, and reportedly mounted cyber attacks to muzzle websites sympathetic to or controlled by Chechen rebels. Some Russian strategic writers view these successes by the Kremlin as a model.

Accordingly, the publicly-released version of Russia's new military doctrine, published in 2010, notes the importance of using IO tools not just to degrade an adversary's command-and-control functions, but to help create a positive view of Russia's actions. It suggests in particular an acute need for "prior implementation of measures of information warfare"—*in advance* of a conflict, in peacetime—in order to potentially "achieve political objectives without the utilization of military force." Such tools are also to be used *during* a war "in the interest of shaping a favorable response from the world community to the utilization of military force" by Russia. The document declares it a national security priority to "develop forces and resources for information warfare" as thus understood.

The Russian Interest

This context is critical for understanding Russia's approach to cyberspace issues, both domestically and abroad. The Russian government's initial encounters with the Internet during the 1990s were apparently characterized by fairly traditional attempts at direct censorship and regulation. Agencies were created to monitor and guide development of Internet-related industry, to delineate and then qualify citizens' rights as they apply in cyberspace, and to impose the ability for state security services to monitor the content of e-mail. (Service providers that did not cooperate had a tendency to be forced offline, as a result of problems with "licensing.")

But when Vladimir Putin ascended to power, the Russian government's approach to controlling online content became more sophisticated. Marcus Alexander of the London Business School has characterized this approach as a sort of "third way" between heavy-handed traditional censorship-based control and U.S.-style Internet liberty. It is a new model by which "an undemocratic government enters competition for maintenance and propagation of its image and power among its population," by embracing and participating in the creation of online content, and by using its power to shape the landscape of available content providers. This conception fits well with the analysis offered by Evgeny Morozov, who has chronicled how authoritarian governments are learning to manipulate the Internet in ever more sophisticated ways for the surveillance and harassment of dissident activity, the dissemination of propaganda, and the

encouragement of popular outlets and diversions that steer citizens away from political expression that is threatening to the regime.

It seems impossible to disentangle such efforts from Russia's post-Soviet conceptions of information operations. The Kremlin's "Information Security Doctrine" (ISD), created in 2000, clearly roots government efforts at domestic information control in considerations of Russian "national security." Among the items in a long litany of potential threats to "information security," the ISD lists "degradation of spiritual values, propaganda of models of mass culture based on the cult of violence, and on moral values contradictory to values accepted in Russian society"; "weakening the spiritual, moral, and creative potential of the Russian peoples"; and "obstruction of the state mass-media's efforts to inform Russian and foreign audiences." Such threats, it says, can originate from foreign sources—among them "the intent of a number of countries to dominate the global information infrastructure." But they can also come from domestic sources, such as "insufficient activity of federal and regional agencies of the Russian Federation in informing the public about their activity, in explaining decisions, [and] in forming government information resources." Among the information threats that present "the greatest danger to spiritual life" in Russia are declared to be "the uncontrolled expansion of the foreign mass media in the domestic information sector" and "the inability of Russia's modern civil society to ensure the young generation's development of constructive moral values, patriotism, and civic responsibility for the fate of the country." Clearly, therefore, the Russian state has a very broad idea of "information security."

This doctrine has become, in its own way, emblematic of the Putin era and the advent of Russia's new governing elite of *siloviki*, political leaders drawn from the ranks of the security services. And it seems to reflect deep fears of the penetration of Russian society by subversive foreign ideas. It is animated, as Thomas has noted, by a clear perception of the importance of preventing "unlawful information and psychological influences on the mass consciousness of society and the uncontrolled commercialization of culture and sciences." As Douglas Carman observed in his March 2002 comment and translation of the ISD in the *Pacific Rim Law & Policy Journal*, the ISD broke new ground insofar as it clearly swept within its ambit "forms of information not normally conceived of in terms of security issues," thereby making them seem like legitimate subjects for state control in the interests of national security.

Russian concepts of information operations, therefore, are wrapped up with the fundamental insecurity of the *siloviki* state as it encounters the

informational anarchy of the Internet. Through Russian eyes, notions of using cyberspace to accomplish the perceived national security interests of the state stretch from the most immediate circumstances of computer network attack to the grandest levels of politico-moral manipulation. "Information security," a term that to American ears tends to signify little more than securing the integrity of our equipment and systems against attack, means much more in Russian usage: it is a sweeping concept tied to the state's need for control over the information space of its citizenry. Russian proposals to ban or regulate cyber weapons cannot be separated easily, or at all, from the authoritarian state's imperative of maintaining domestic political control.

The common belief that Russia fears a cyber arms race with the United States is accurate. Some Russian officials have said as much—even fretting that Western technological breakthroughs mean that it would be an arms race in which Russia could compete but would be unlikely to win. It is not nearly as widely understood, however, that when Russian officials imagine such possibilities, they envision more than simply a technical competition in attacking or defending computer-based systems. Their fear of cyber attack is inseparable from a deeper dread of political subversion associated with the free flow of information. It is therefore to be expected that any Russian proposals for a new international "information security" regime will seek to address both such perceived threats.

Chinese Concepts of Cyberwar

What writings are available on China's conception of cyber conflict suggest that some elements of Chinese thinking parallel American ideas of fighting and defending against attacks over computer networks. But Beijing's overall conception of cyber conflict is, like Russia's, bound up with the control of information and the manipulation of adversaries' views and decision-making processes. As in the Russian doctrine, this manipulation is meant to occur not just in wartime, but also—and especially—during peacetime, when it can aid either in ensuring the maintenance of a favorable peace, or in achieving victory without actually having to fight.

Echoing themes in China's ancient statecraft literature, for instance, modern Chinese writings say that the objective of information warfare is to subdue the enemy without a battle, and to trick him into adopting your goals as his own. In this context, information "weapons" are aimed at the enemy's understanding of the world; his basic convictions and beliefs are the "target" of attack. Not surprisingly, therefore, some Chinese writers

identify communications and the media as the main strategic focuses, suggesting that the key to success lies in a state's ability, as Timothy Thomas puts it, "to gain the initiative over information resources and control of the production, transmission, and processing of information so as to damage information-based public opinion on the enemy's side." This attitude may be reflected in the remark of one unidentified Chinese general, quoted by CIA official John Serabian in testimony before Congress's Joint Economic Committee in February 2000, that the objectives of cyber attack included not only penetrating computer systems and transmitting disinformation to enemy military leaders, but also using cyber tools to "dominate" the enemy's "entire social order."

This focus of modern Chinese information warfare theory self-consciously echoes Maoist concepts of a "People's War." As one Chinese author put it in a 1996 paper, "anybody who understands computers may become a 'fighter' on the network," making possible simultaneous mass attacks "carried out by hundreds of millions of people." Consequently, "information-related industries and domains will be the first to be mobilized and enter the war."

As in Putin-era Russia, this understanding of the sociopolitical breadth of information warfare bespeaks China's fear of "information attack" at least as much as any aspirational capability to attack others. Beijing, in short, worries greatly about subversion through uncontrolled mass access to information. As also with Russia, Chinese approaches to cyberwar and cyber arms control therefore cannot be disentangled from the national security threat the Chinese regime believes to be presented by unchecked popular access to information. As explained in the English-language version of the Chinese government's official declaration of Internet policy, a white paper released in 2010, the state aims to ensure "a healthy and harmonious Internet environment" by bringing "law-based administration and ensured security" to cyberspace. The regime admits to attaching "great importance to social conditions and public opinion as reflected on the Internet." This reflects Beijing's determination to shape those opinions by controlling the substantive information accessible by Chinese citizens online.

As the white paper takes pains to point out, it is a "basic principle" of China's Internet policy that "no organization or individual may utilize telecommunication networks to engage in activities that jeopardize state security, the public interest or the legitimate rights and interests of other people." Moreover, the state aims to employ "technical means… to prevent and curb the harmful effects of illegal information on state security, public

interests and minors." For instance, Chinese law prohibits "the spread of information that contains contents subverting state power, undermining national unity, infringing upon national honor and interests, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror, or other information that infringes upon the legitimate rights and interests of others." China's list of illegal online content is extraordinarily broad, and it seems almost infinitely malleable:

> No organization or individual may produce, duplicate, announce, or disseminate information 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.

This lengthy recital gives a taste of the rationale for the so-called "Great Firewall of China," an extraordinary cyber-management project whereby the government in Beijing has sought (with mixed success) to carve a *de facto* "Chinese" Internet off from the rest of the global information system. Or, to be more precise, the aim appears to be not so much to have an entirely "separate" Internet, but to police a Chinese zone *within* the global information system in which certain types of disapproved, politically-related information and activity cannot appear. On the basis of the policy parameters announced in the white paper, and operating in the name of social "harmony," the Chinese Communist Party goes far beyond conventional efforts to suppress such things as cyber fraud and child pornography, policing the frontiers and internal terrain of its sovereign Internet landscape to ensure the suppression of content deemed subversive to state policy.

Making Islands of the Internet

Although the Russian and Chinese conceptions of information control and war may seem distant from the much more technical American conception of cyberwar, they are nonetheless essential to evaluating proposals for cyber arms control. Such proposals are really only just beginning to

be aired, as Russian and Chinese officials play to the Western instinctive preference for legalistic, treaty-based approaches to solving international security problems.

Moscow has argued for an international prohibition upon information weapons, and has promoted the idea, including at the United Nations, in order to shape an international understanding of the world's options in dealing with cyber threats. Such overtures are not separable from the broader Russian concerns about the uses of information. In the words of Sergei Ivanov, a high-ranking Russian official who was minister of defense from 2001 to 2007, Russia wants to develop "international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security."

For their part, Chinese officials demand that Western countries respect their interpretation of what information security means. Observing that "national situations and cultural traditions differ among countries, and so concern about Internet security also differs," Beijing's white paper declares that "concerns about Internet security of different countries should be fully respected." The white paper also evinces a deep concern for sovereignty. "The Internet sovereignty of China should be respected and protected," it says, presumably meaning that China should have legal protection from Internet-facilitated information attacks *as China interprets them.* But China's interpretation of information attacks includes, as we have seen, the transmission of subversive political thought or cultural content. Also, in keeping with Beijing's efforts to recover control over an Internet-based information space notoriously resistant to the very idea of national frontiers, China wishes to bring the Internet under a system of political regulation. "China holds that the role of the U.N. should be given full scope in international Internet administration," the white paper says. "China supports the establishment of an authoritative and just international Internet administration organization under the U.N. system through democratic procedures on a worldwide scale." When speaking of the U.N. process as lived out between sovereign states, the phrase "democratic procedures" seems in fact to mean one-country-one-vote majoritarian control—which would bring the Internet under the supervision of some multilateral political organ roughly analogous to the General Assembly.

Similarly, as Douglas Carman explained in his analysis of Russia's Information Security Doctrine, Moscow's approach is predicated not merely upon a broad concept of information conflict, but upon an idea that analogizes cyberspace to a country's physical territory: "Applying this

physical metaphor of legal doctrine to a conceptual landscape, or 'information space,' this contemporary interpretation of sovereignty suggests the ultimate authority of the nation-state to regulate its information and media networks." In both Russian and Chinese approaches to "information security," therefore, one can see a consistent conceptual thrust: an attempt to *re-territorialize* the Internet into islands of national sovereign political control. If anything, China's white paper, with its explicit invocations of the importance of "respect" for China's Internet "sovereignty" and its defense of the Great Firewall, makes this focus even more clear. Perceiving threats to regime security in the openness of modern cyberspace, both governments wish to acquire something of the sovereign control over the Internet that their countries still enjoy with respect to physical geography.

Avoiding a Trojan Horse

The idea of cyberspace arms control is now still very much up in the air, with observers sharply divided over Russia's proposals. In July 2010, a U.N. panel on this subject—convened in 2005 to help break what the *New York Times* called "an impasse of more than a decade between the United States and Russia over how to deal with threats to the Internet"—finally issued its long-awaited recommendations. They broke little new ground, however, simply calling for more diplomatic discussions to share information about different national approaches to computer security legislation, the protection of computer networks, and the use of computer and communications technologies during warfare.

Calls for further discussion and debate over cyber arms control will surely continue, and there may be valuable steps that can be taken—especially in connection with improving cooperative procedures for coping with the effects of cyber assaults, reconstituting information systems in their aftermath, and determining the source of an attack. In this regard, we might take our cue from the Council of Europe's Convention on Cybercrime, ratified by the United States in 2006, which obliges governments to adopt their own national legal measures to facilitate the investigation and prosecution of criminal activity carried out in and through cyberspace.

It might also be possible to strengthen international understandings of cyber attack as being legally equivalent to other forms of destructive hostility. Indeed, Obama administration officials made just such a suggestion to the U.N. panel, arguing that, in the words of one diplomat, "The same

laws that apply to the use of kinetic weapons should apply to state behavior in cyberspace." It may be advisable for states to clarify that longstanding principles of the law of armed conflict do indeed apply in the cyber arena to attacks directed at information or physical systems. It may be possible, furthermore, to offer more coherent articulations of an international cybersecurity regime that focuses on attribution, deterrence, and possibly even preemption. Such a strategy should emphasize the fact that cyber assaults can trigger collective security responses. It may even be possible, as former U.S. Director of National Intelligence Mike McConnell has suggested, to gradually modify Internet technical protocols in order to improve the system's ability to identify the sources of an attack.

As with the EU's Convention on Cybercrime, however—which included a protocol calling for content restrictions, in the form of a ban on "racist" speech, that the United States refused to ratify for fear that it would facilitate political content restrictions—we must be wary of attempts to regulate substantive Internet content that could be smuggled in under cover of urgent efforts to improve cooperation against legitimate threats. The authoritarian regimes that presently hold power in Moscow and Beijing conceive of information warfare as involving significant elements of socio-cultural subversion, carried out through the Internet and mass media outlets, that go far beyond the conveyance of malicious code or disruptive technical signals, and that reach into the realm of political ideas. These governments feel themselves to be threatened by just such ideational attack, and they seem to approach Internet regulation in their own societies from the perspective of ensuring "security" against "information weapons" of this very sort. These perspectives cannot be entirely separated from their proposals for cyber arms control.

None of this means, of course, that Russian and Chinese officials are incapable of proposing cyber arms control initiatives that are genuinely useful and constructive—initiatives that it would be in the interest of the United States to support. We clearly do face enormous threats from cyber attack, and if arms control approaches can help lessen them, we would be remiss were we not to consider such measures, or indeed to propose good ones ourselves. But the distinct, opposing, and potentially misleading interests of other nations should make our initial stance toward such suggestions be one of caution, even while we remain open to constructive possibilities.