REACTION

CYBERDETERRENCE

Robert F. Turner[*]

Messrs. Kohlmann and Bijou are certainly correct in identifying cyberattacks as rapidly emerging threats to the United States' national security. They have made a valuable contribution to one of the most important issues of our era.

The term "cyber" denotes some relationship with computers, and thus encompasses a broad range of activities that cannot be addressed in a single manner. Seizing control of a military command network to launch lethal attacks, modifying the mixture of ingredients at a baby formula manufacturing plant in order to poison innocent infants, or attacking critical infrastructure networks to endanger large numbers of human lives, may well warrant a military response pursuant to the Law of Armed Conflict (LOAC) paradigm. Collecting intelligence information by hacking into government computer systems or stealing trade secrets from U.S. corporations to benefit foreign competitors, might warrant nonviolent responses.

Whatever the source, intent, or nature of the attack, one thing is clear: America needs to enhance its cybercapabilities so that it will be able to detect and respond effectively to attacks. Equally clearly, the most effective responses will focus on affecting the perceptions of decisionmakers on the other side. Put simple, *incentives matter*.

Individuals — whether government officials, foreign terrorists, or corporate executives — make decisions based upon cost-benefit perceptions. Understanding those perceptions, and finding ways to modify them, is at the core of deterring attacks. This reaffirms the importance of being able to identify the actual source of a cyberattack. Unless that identification can be done, America's ability to deter or punish such behavior will obviously be limited.

For all of its bluster, Iran is not likely to launch a direct lethal attack against America — whether by missile or computer — because its leaders understand that the U.S. government's ability to respond with lethal force greatly exceeds Iran's. But if they believe they can mask

---

[*] Professor Turner holds both professional and academic doctorates from the University of Virginia School of Law, where in 1981 he co-founded the Center for National Security Law. He is a former three-term chairman of the ABA Standing Committee on Law and National Security, and for many years edited the ABA *National Security Law Report*.

the attack as originating from Israel or some amorphous transnational terrorist group, all bets are off.

Deterrence will also fail if an adversary concludes the United States lacks the *will* to respond effectively to cyberattacks. For this reason, it may be useful to demonstrate that resolve at an early date — to make an example of someone who miscalculates America's ability or willingness to respond decisively to cyberattacks.

The goal of sanctions — whether in the form of economic sanctions or a responsive cyberattack — should be to inflict maximum discomfort upon decisionmaking elites, while in the process inconveniencing the innocent as little as possible. Applying the principle may not always be easy, but it is nevertheless an important goal.

While there are circumstances in which cyberattacks may warrant a military response, the United States has a broad range of options and need not limit itself to more traditional responses. Consistent with the U.S.'s treaty obligations, damage to American economic interests might be met by diverse counterattacks — including legal proceedings or covert measures to seize the contents of bank accounts belonging to those responsible for the attacks. Ideally, the United States should explore the option of providing for such remedies by international treaty, and limited progress has been made in this direction — particularly in NATO and the Council of Europe. The need to find new approaches is not exclusively an American problem; the more the world community can unite behind effective countermeasures, the better. If the United States is to demand that other countries take action against their citizens or others within their territory who launch cyberattacks against American targets, it should lead by example by imposing serious criminal penalties for comparable actions by those subject to U.S. jurisdiction.

As perhaps minor quibbles, I would urge the authors to avoid describing contemporary international legal norms governing the use of force (*jus ad bellum* and *jus in bello*) in terms of "just war" theory — as the U.N. Charter clearly rejected key tenets of that doctrine (such as justifying war for the propagation of faith). Nor is force justified by the existence of an "imminent threat" — life is filled with potentially "imminent" *threats* (any powerful neighbor able to attack without warning might be perceived as an imminent threat) — but, to justify the use of force in "anticipatory self-defense," there must be clear evidence of an imminent *attack*.

Even if it were possible to draw a clear line between "American" private companies and those belonging to foreign nations or their citizens, the authors are certainly correct that having NSA "working on behalf of private companies" would be "troubling." For generations, freedom-loving people around the world have (often at considerable personal risk) provided valuable data to American intelligence services. Many sources of such information might quickly dry up if there

was a perception their information might simply be used to promote private American commercial interests.

But it does not follow that the U.S. government ought not use the NSA and other intelligence agencies to identify foreign threats to the intellectual property rights of Americans, particularly when those threats are directed or assisted by foreign governments. To mention one example, for years French intelligence agents have surreptitiously entered the hotel rooms of American corporate officials attending the Paris Air Show to search for documents to copy and share with French corporations. These efforts led to calls for similar support for U.S. corporations from the American intelligence community.

A wiser approach, in my judgment, would be for the American intelligence and counterintelligence communities to ascertain the existence of such activities, and to work through the State or Commerce Departments to alert business travelers of potential risks they may face during their travels (along with unusual health or physical security risks). In addition, I have long felt that diplomats might have a candid discussion with host governments who engage in such behavior, informing them that the United States is aware of their efforts to steal intellectual property (whether via photographing the contents of briefcases left in hotel rooms or hacking into corporate web sites), and views it as unacceptable. If the thefts continue, the United States may find it necessary to unleash its own intelligence services to acquire the most sensitive intellectual property secrets of corporations from the offending countries and surreptitiously post them on the Internet for all of their competitors to view.

The basic message would be that America will not use its military or intelligence resources to violate the rights of other nations or their citizens, but has tremendous ability to do harm to those nations that violate the U.S.'s rights or permit those under their jurisdiction to do so. Countries will continue to use both traditional means and new computer technologies to try to acquire intelligence information, and corporations will no doubt continue to try to steal secrets from their competitors — at home and abroad. As the United States too will continue to spy on other governments and U.S. citizens will no doubt engage in corporate espionage, the nation needs to establish and enforce reasonable standards of behavior — perhaps by treaties or other international agreements. And if the United States demands that foreign governments and those within their jurisdiction cease cyberattacks on our government or citizens, the U.S. government must take reasonable measures to uphold the same standards of conduct by those within its jurisdiction.

Establishing standards in advance, and working with other governments to enhance America's ability to identify the actual source of threats to our security, are obviously desirable. I see no benefit, however, in announcing a minimum threshold for action, as doing so will

incentivize lower levels of cybermisconduct. It should be clear that using a keyboard to accomplish a result that, if done by more traditional means, would justify a military response will not change the outcome. Hacking into American computer systems to undermine the nation's military readiness or to endanger the safety of its citizens will result in a response that — when the dust settles — will make the perpetrator far worse off than before the attack. Whether done by tampering with the setting of a water treatment plant using a laptop from 6,000 miles outside the borders, or cutting a padlock to pour poison directly into the water supply, the tragic consequences may well be the same. The United States must make it clear to all that it reserves the right to use necessary and proportional force — including lethal military force — in response to such activities.