Testimony

Managing September 12th in Cyberspace

Martin C. Libicki

RAND Office of External Affairs

CT-383

March 2013

Testimony presented before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on March 20, 2013

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

Martin C. Libicki[1]
The RAND Corporation

Managing September 12th in Cyberspace[2]

Before the Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
United States House of Representatives

March 20, 2013

On September 11th, 2001, terrorists attacked the United States. Three thousand people died and the physical damage was upwards of two hundred billion dollars. On September 12th, the country responded. The United States strengthened its homeland security. We went to war twice. Over the next dozen years, the United States lost six thousand in combat. Ten to twenty thousand were seriously injured. Total additional expenditures exceeded a trillion dollars. I point this out not to criticize the policies that followed – but to indicate that even though an attack on the United States may be damaging, the cycle of response and counter-response may be far more consequential.

Accordingly, even though a cyber-9/11 may be costly, it would be shortsighted to evaluate the threat in terms of immediate damage without considering how the United States would manage such a crisis in order to yield an outcome that works best for the American people. That is, we are right to be worried about a "9/11 in cyberspace," but we also ought to worry about what a "9/12 in cyberspace" would look like. Indeed, one of the best reasons for working hard to avoid a 9/11 in cyberspace is avoid having to deal with a 9/12 in cyberspace. That noted, because a cyber 9/11 (or what looks like a 9/11) might happen, it is worthwhile to think about what we do the day after.

The issue of how the United States should manage crisis and escalation in cyberspace is addressed in the recently-published RAND document of that name.[3] I now want to take the opportunity to touch on some of the salient points in that document, as well as follow-on thoughts.

The first point is to understand that the answer to the question – *is this cyberattack an act of war?* – is not a conclusion, but a decision. In physical combat, such a question may be meaningful: if

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT383.html.
[3] Martin Libicki, *Crisis and Escalation in Cyberspace*, Santa Monica CA (RAND), MG-1215-AF.

your neighbor's tanks are in your backyard heading for the capital, then war is on. But such a question is usually the wrong one to ask about cyberwar. True, cyberwar can disrupt life even on a mass scale. Cyberwarfare can enhance conventional military power. But, it cannot be used to occupy another nation's capital. It cannot force regime change. No one has yet died from it. And, Stuxnet notwithstanding, breaking things with ones and zeroes requires very particular circumstances. A cyberattack, in and of itself, does not demand an immediate response to safeguard national security. Instead, a country struck from cyberspace has the opportunity to ask: What would be its most cost-effective way to minimize such future suffering? If war fits the bill (and other nations understand as much), the victim of a cyberattack could declare that it was an act of war and then go forth and fight. Perhaps making war can persuade the attacker to stop. Yet, war also risks further disruption, great cost, as well as possible destruction and death -- especially if matters escalate beyond cyberspace. Or a country may look at policies that reduce the pain without so much risk – such as by fixing or forgoing software or network connections whose vulnerabilities permitted cyber-attacks in the first place.

Second is to take the time to think things through. Computers may work in nanoseconds, but the target of any response is not the computer – in large part because even if a computer is taken out a substitute can be close at hand. The true target of a response is those who command cyberwarriors – that is, people. But, people do not work in nanoseconds. Persuasion and dissuasion of people work at roughly the same speed whether or not these people command cyberwar or any other form of war. A corollary error is to assume that a confrontation in cyberspace is inherently unstable – thereby necessitating being a quicker draw than the other guy. It is precisely, because unlike with nuclear war, a nation's cyberwar capabilities cannot be disarmed by a first strike, there's not the same need to get the jump on the other guy, just as there is not the same need to match his offense with your offense, when it's your defense that dictates how much damage you are likely to receive.

Third is to understand what is at stake – which is to say, what you hope to gain by making the attackers cease their efforts. This goes for both responding to cyberattack and responding to what might be deemed intolerable levels of cyber-espionage. With cyberattack, what you are trying to prevent is not the initial attack, but the next attack – the effects of which might be larger than the initial attack but may also be smaller. (This is particularly true if the initial attack teaches the immediate victims, that, say, making industrial controls accessible to the Internet may not have been the smartest idea.) As for espionage, we really have no handle on how to evaluate the damage that takes place to the country when other countries see what we don't want them to see.

Fourth is not to take possession of the crisis unnecessarily – or at least do so only on your own terms. That is, do not back yourself into a corner where you always have to respond, whether doing so is wise or not. It is common, these days, to emphasize the cost and consequences of a cyberattack as a national calamity; last week the Director of National Intelligence proclaimed it as the primary short-term threat to the nation. Making such arguments tends to compel the United States to respond vigorously should any such cyberattack occur, or even merely when the possible precursors to a potential cyberattack have been identified. Having created a demand among the public to do something, the government is then committed to doing something even when doing little or nothing is called for. In some cases, it may be wiser to point out that the victim had a feckless cybersecurity posture. In other cases, downplaying the damage may be called for. The more emphasis on the pain from a cyberattack, the greater the temptation to others to induce such pain -- either to put fear into this country or goad it into a reaction that rebounds to their benefit. Conversely, fostering the impression that a great country can bear the pain of cyberattacks, keep calm, and carry on reduces such temptation. Correspondingly, despite good arguments in favor of drawing red lines for deterrence purposes – "if you do this, I will surely do that" – the cost of being credible is that if deterrence fails, such a declaration tends to constrain one into carrying out retaliation. To do nothing or nothing much, at that point, tends to hollow all deterrent postures, and not just in cyberspace. Given the inevitable ambiguities associated with the consequences and causes associated with cyberattacks, inflexibility may also demand a response well before the facts are clear. There are careful tradeoffs that have to be made.

Fifth is to craft a narrative that facilitates taking the crisis where you want to take it. Narratives are, essentially, political morality plays, in which the United States has to select a role that puts it in a good light while retaining basic consistency between the facts of the matter, as well as with its previous narratives. Part of crafting a narrative requires finding the right role: does the United States want to portray itself as a victim of cyberattack? As the righteous enforcer of international norms? As the superpower that demands respect? Narratives also have to find a role for the attacker, and the definition of such a role may, in some cases, have to encourage and accommodate the attacker's graceful and face-saving retreat from belligerence. After all, the odds that an attack in cyberspace arises from , miscalculation, inadvertence, espionage with unintended consequences, or the actions of a rogue actor are nontrivial.

Sixth is to figure out what norms of conduct in cyberspace, if any, work best for the United States. Last week both the United States and China agreed to carry out high-level talks on cyber norms. Although nearly four years of Track II negotiations with the Chinese (in which I participated) have yielded meager results, there are still some grounds for optimism. But, first we have to address some salient questions. To what extent can the Laws of Armed Conflict apply in a domain where

the patterns of collateral damage are poorly understood, where the distinction between civil and military is difficult to discern, where it's getting harder and harder to know where your information sits, and where the transparency required for neutrality simply does not exist? Where does one draw the many lines among cyberwar, cybercrime, cyber-espionage, and violations of international trade rule? Is it in the U.S. interest to make unconstrained espionage a *casus belli*? How well should states be able to monitor (let alone enforce) compliance before it can assure itself that the norms are worth having?

Seventh is to manage cyber-escalation wisely. This not only means remembering that the other side will react to what you do, but also understanding what a crude tool counter-escalation may be for influencing the other side. Consider that with Stuxnet, it took many tries to get the desired effect. The Iranians may not have known they were under attack until they read about it in the *New York Times*. It is also unclear whether we would have had much damage assessment had the centrifuge plant not been under independent inspection. To further illustrate what the fog of cyberwar may mean to escalation control, assume a defender wants to place in an opponent's mind the thought that if he escalates and the defender will counter-escalate proportionally. But in cyberspace what the attacker does, what he thinks he did, and what the defender thinks he did may all be different. The defender can only react to what he thinks the attacker did. That is because the defender's systems are usually different than the attacker's. Equivalence between perception of the attack and the intended response may be inexact. Then there's the similar difference between the defender's response and the attacker's perception of what was done in return. After all this, the attacker may think the retaliation was proportional, understated, or went overboard in crossing counter-escalation red lines -- redlines that were not originally crossed by himself. The effect is akin to playing tennis on a rock-strewn court.

In sum, while I believe it is certainly worthwhile effort to prevent a future 9/11 in cyberspace – and understanding the nature of the threat is an important component of that effort – similar levels of care and thought needs to be given to how to manage a potential 9/12 in cyberspace. If not, we may find, as with the historical 9/11, that the consequences of the reaction and counter-reaction are more serious than the consequences of the original action itself.