Heritage Lectures

Published by The Heritage Foundation

No. 1123
Delivered May 19, 2009

June 12, 2009

# The Confluence of Cyber Crime and Terrorism

*Steven P. Bucci, Ph.D.*

Today the world faces a wide array of cyber threats. The majority of these threats are aimed at the Western democracies and the Western-leaning countries of other regions.

The reason for this is simple: They are ripe targets. These countries are either highly dependent, almost completely in some cases, on cyber means for nearly every significant societal interaction or are racing toward that goal. They seek the speed, accuracy, efficiency, and ease that a "wired" system of systems brings and all the benefits that accrue to such a situation.

The danger we face is that there are many individuals, groups, and states that desire to exploit those same systems for their own purposes. There is a new threat on the horizon that must be recognized and addressed.

Cyber threats we face today can be grouped into seven categories that form a spectrum of sorts. (See Figure 1.) Any of these threat groups can attack an individual, a nation-state, and anything in between. They will exploit a lazy home computer user, an inefficient corporate information technology system, or a weak national infrastructure defense.

## Levels of Danger

We are all in danger from these threats, which can be grouped as low, medium, and high levels of danger. Any construct of this nature is a simplification, but it does aid in discussions to have the numerous possible actions defined into manageable groups.

## Talking Points

- The West has a huge number of intelligence and law enforcement assets dedicated to stopping the proliferation of weapons of mass destruction but does not have the same type of watchdog systems in place to prevent cyber enablement.
- Terrorists are very good and getting better at using the Internet for propaganda and fundraising. They are reaching ever-increasing audiences.
- Terrorists will recognize the opportunity the cyber world offers and that they need help to exploit it. The highly developed cyber criminal networks want money and care little about the source.
- Unless we get cyber crime under control, it will mutate into a very real national security issue with potentially catastrophic ramifications. Terrorism enabled by cyber criminals is our most likely major cyber threat.

This paper, in its entirety, can be found at:
*www.heritage.org/Research/NationalSecurity/hl1123.cfm*

Produced by the Douglas and Sarah Allison
Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis
Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

At the low danger end, there are two groups of threats. The lowest level is the individual hacker. He operates for his own personal benefit: for pride, self-satisfaction, or individual financial gain. He constitutes an annoyance. The hacker category also includes small groups who write malware (malicious software) to prove that they can or who attack small organizations due to personal or political issues.

With the hacker at the low end of the spectrum are small criminal enterprises and most disgruntled insiders. These too are low-level annoyances, except for the unfortunate individuals they exploit as their primary targets. These operate Internet scams, bilking people out of personal information, and may even perpetrate extortion through threats.

Continuing along the spectrum, the medium-level threats are harder to break down in a rank order. Each threat grouping targets different entities. These targets would consider their attackers very dangerous and a critical threat. These medium-level threats include:

- Terrorist use of the Internet;
- Cyber espionage, which is also helped by insiders at times, both corporate and national security types, including probes for vulnerabilities and implementation of backdoors; and
- High-level organized crime.

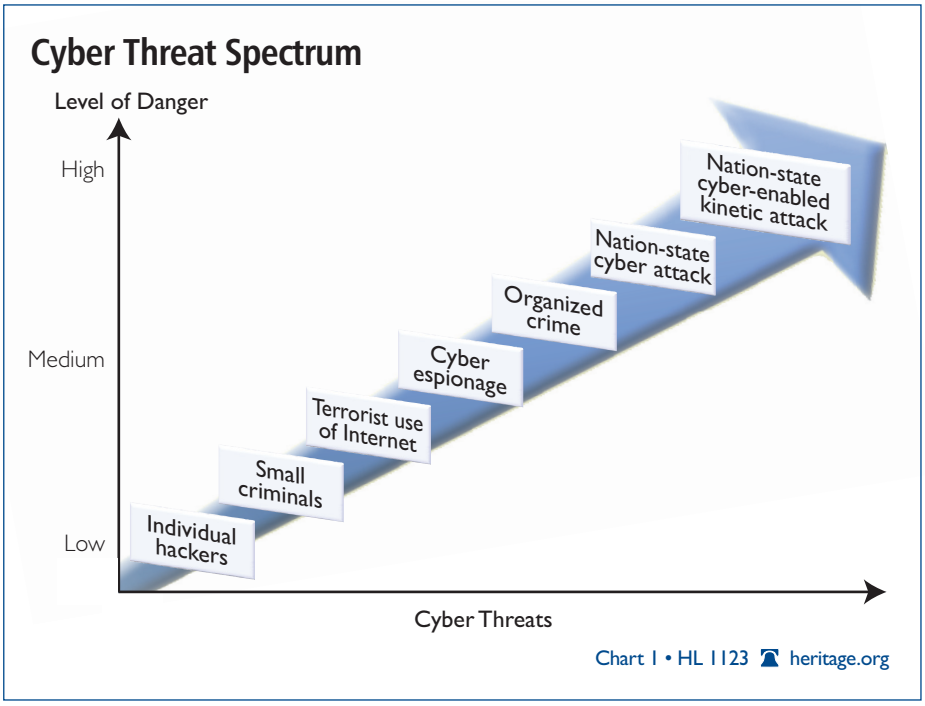
All three of these groupings can have extremely detrimental effects on a person, a business, a government, or a region. They occur regularly and define the ongoing significant threats we face every day.

The high-level threats involve the full power of nation-states. These come in two major groups. The first is a full-scale nation-state cyber attack. The closest example of this was the assault made on Estonia in 2007. There, the highly developed network of a small country was temporarily brought to its knees. Portrayed by some as a simple display of public outrage over the moving of a statue, most felt there was more going on and that a government hand was at play.

This dispute over the responsibility makes this an imperfect example, but it is a highly troubling harbinger of the future. One former Department of Defense (DoD) leader stated that over 1 million computers were used in this event, coming from over 70 countries.

The other possibility is the cyber enablement of a kinetic attack. So far, we can only look to the 2008 assault on Georgia to study this category. Georgia was not as dependent on the cyber realm as was Estonia, but the cyber assault that preceded the Russian military's ground attack into Ossetia severely hindered Georgia's response. Again, it may be an imperfect example, but it has given us much to consider. The same former DoD official described it this way:

> [T]heir cyber special operations forces isolated the president by disabling all his cyber connectivity, then their cyber air force carpet bombed the entire national network, and finally their cyber Delta Force infiltrated and rewrote code that kept their network from



working correctly even after it was brought back up. It was a highly sophisticated attack.

These two potential threats constitute the high end of the cyber-threat spectrum.

## A Construct for Planning

During the Cold War and beyond, the military and security communities used a paradigm for planning that allowed them to determine against which of a large number of possible threats they should plan. They would determine both the *most dangerous threat* and the *most likely threat*. These were seldom the same.

During that period, there was near-universal agreement that full-scale thermonuclear exchange between the U.S. and NATO on one side and the Soviet Union and the Warsaw Pact on the other was the most dangerous threat. Fortunately, this was not the most likely threat. Mutually assured destruction kept the fingers off the triggers.

Planners therefore had to ascertain what scenario was the most likely. For NATO, this was a large-scale conventional war on the plains of Northern Europe, which all hoped would remain non-nuclear. For the U.S., they added smaller-scale proxy wars outside the European context. Today, we can use a similar process to help us thoughtfully address cyber threats.

While we face a scenario emerging from the cyber-threat spectrum that fully fits the part of the most dangerous threat, we must also face and prepare for a most likely scenario that is unique and, frankly, is not yet on the cyber-threat spectrum. This threat will involve the joining of the growing cyber-crime capability we see today with the terrorists' realization that the cyber realm is ripe for exploitation and that joining with cyber criminals will be their path to that exploitation.

## The Most Dangerous Cyber Threat: Nation-State Attacks

Clearly, as one looks at the spectrum of threats, the far end delineates the possibilities we fear most. Developed nation-states, acting as peer competitors, are the most dangerous potential threat.

Nation-states possess hard power, including kinetically capable militaries, economic strength, industrial bases, and scale of assets. They can marshal the intellectual capital to develop cyber armies—large numbers of operators with the best equipment, skilled at developing and using new forms of attack. These will do the twin tasks of both leveraging and enabling conventional intelligence, signals, and mobility assets.

Nation-states can also use their considerable coercive powers to harness civilian assets that technically fall outside the public sector. This can be done by requiring active or passive collusion with the government or by manipulating public sentiment to stir up patriotic fervor while providing guidance (i.e., targeting) and tools to the faithful.

All of the above factors allow nation-states with foresight to develop and use enormous capabilities in the cyber realm. What is today merely cyber espionage or probing of defenses can, in the blink of an eye, be turned into a massive attack on the infrastructure of an adversary.

Remember: Cyber forces do not need to deploy by ship, plane, or truck, so there are no logistical delays or the usual indicators and warnings. Cyber attacks could be used to disable defenses and blind intelligence capabilities in preparation for a devastating kinetic strike. These methods can slow the reactions of defenders by clouding their operation picture or fouling their communications means. Cyber attacks could bring down key command and control nodes altogether, paralyzing any response to the attack.

If the attacker has used weapons of mass destruction (chemical, biological, radiological, nuclear, and high-yield explosives) in the kinetic part of the attack, the cyber component can also hinder the ability to rally consequence-management assets. The victim will have suffered a catastrophic attack and will be unable to respond effectively to the results. The continued cyber intrusions will not only keep them from striking back with any real effect, but may make them ineffectual in mobilizing their first-responder forces.

This kind of large-scale attack can only come from a nation-state and obviously constitutes our most dangerous scenario. It is very fortunate that it is also not a very likely one.

The reason is old-fashioned deterrence. In the same way our cyber and physical infrastructures make us vulnerable to this scenario, any attacking nation-state must have its own infrastructure capabilities to be able to execute it. Those cyber capabilities and kinetic forces used in the attack are also potential targets, as is the remainder of the attacker's critical infrastructure.

Basically, it is unlikely that a nation-state would do this, because they also have much at stake. Deterrence, in the same way we have understood it for over 50 years, still applies to nation-states in all the ways it does not apply to terrorists, criminals, and other non-state actors.

A large-scale cyber attack or cyber-enabled kinetic attack by a peer competitor on another country runs the risk of a large-scale response from the target or the target's allies and friends. While this will not dissuade every nation-state–backed cyber threat—the thousands of probes, minor attacks, and espionage actions prove that—it has continued and will continue to keep this type of nightmare scenario from moving into the "likely" category. Yes, we must prepare for it, but if this is the only thing we prepare for, we will have failed our countries.

One final thought on this subject: Opinion leaders might point to the situations in Estonia and Georgia mentioned earlier as evidence that deterrence did not work in 2007 and 2008. Friendly nations must explicitly state their intentions to protect and support one another from this sort of attack in the same way we did during the Cold War; without a strong declaratory policy of mutual defense in cyber situations, there will be no deterrence.

If we fail in this, smaller nations will continue to be at risk from larger, more powerful neighbors, and this is unacceptable. If we act strongly and in a united fashion, this will constrain nation-states—but will not constrain terrorists.

## Terrorist Use of the Cyber Realm: From Small Beginnings…

It is fortunate that so far, the major terrorist organizations such as al-Qaeda and its franchises have not yet learned to fully exploit the "opportunities" in the cyber realm. We would be foolish to assume this state of affairs will persist.

Terrorists are limited in their understanding of the potential for this medium. They do use it extensively, but not for offensive actions. Most intelligence and law enforcement agencies agree that they are limited to such areas as communications, propaganda, financial dealings (fund-raising and fund transfers), recruitment, and intelligence. There is some potential use for operational planning and reconnaissance, but it is unconfirmed.

Communications security on the Internet is very attractive to terrorists. The anonymity and difficulty of tracing interactions in restricted, password-protected chat rooms and the use of encrypted e-mails give terrorists a much greater degree of operational security than other means of communications. This will continue to be a major activity for terrorists over cyber channels.

Clearly, the terrorists are very good and getting better at using the Internet for propaganda and fund-raising purposes. The increasing sophistication of their messaging shows an understanding of the potential of the cyber medium in this area. They are reaching ever-increasing audiences. YouTube-like videos of terror attacks feed the fervor of the faithful around the world and make them feel a part of the struggle. Messaging over the Internet from the leadership keeps them prominent in the minds of the mass audience and makes the most isolated spokesperson seem relevant.

These same channels are superb for fund-raising among the dispersed peoples around the world. The reach and timeliness cannot be matched by other communications means and greatly aids in their fund-raising efforts. These same characteristics apply to their recruitment programs, and the process of radicalizing individuals no longer has to take place in person, but can be greatly enhanced by cyber communication and teaching.

There are many very effective applications available that aid in basic intelligence gathering. Google Earth and similar programs can be obtained for free and will give street-view photos of potential targets, as well as excellent route and obstacle information. The tendency of most Western countries to post nearly everything there is to know about critical infrastructures on unsecured Web sites is a great boon to the terrorists and requires no more exper-

tise than an ability to use rudimentary search engines that small children have mastered. All of this "research capability" assists the terrorists in making their standard operation procedures much easier and safer to polish to a high degree.

A new wrinkle that is developing is the use of virtual worlds. There is hard evidence of money transfers having been made within these worlds. This is done by using real cash to buy virtual currency, conducting various transactions within the virtual environment, and then converting it back into real cash again in a completely different temporal location. It is all safe, clean, legal, and nearly impossible to trace.

These virtual worlds also allow for meetings to occur in cyber space that are even more deeply covered and protected than secure chat rooms. The avatars used in virtual worlds are very difficult to identify, and rules for interaction online allow for secret activities that further shield those with much to hide.

An advanced application which has been discussed by intelligence and law enforcement agencies is the use of virtual worlds to train and rehearse for operations in the real world. This is clearly possible, but no hard evidence is yet available to prove that terrorists are now using the virtual worlds in this way.

Someone must lead the terrorists of the world to the next level of cyber capability. It is unlikely that they will develop their own cyber plans and abilities beyond a few experts to ensure they are not being cheated or who can do operational cyber planning correctly. To do more than that would take a great deal of time, and they may be unwilling to wait. Unfortunately, they do not need to wait, as they will probably do it by reaching out to the world of cyber crime. There they will find willing partners.

## Cyber Crime: Follow the Money

Cyber crime continues to be a booming business. What started as an offshoot of individual hackers doing it for fun and pride has grown into a huge (and still expanding) industry that steals, cheats, and extorts the equivalent of many billions of dollars every year. They steal from individuals, corporations, and countries. It does not matter if it is simple scams to get gullible people to give up money and access to their accounts or highly sophisticated technical methods of harvesting mass amounts of personal data that can be exploited directly or sold to others; cyber crime is big money. The more sophisticated it gets, the more organized it becomes, and it has matured to a frightening level.

A lucrative target is data well beyond personal identity and financial information. Infiltrating businesses and stealing industrial secrets, pharmaceutical formulas, and like data can reap huge profits for criminals.

There are several reports of utility facilities having their SCADA (supervisory control and data acquisition) systems hacked and seized by criminals. The attackers have threatened to shut down the facility or worse if they were not paid enormous ransoms. No one knows if the malefactors could have actually followed through on the shutdown threats, as in each case the money was paid. The owners deemed it a credible threat and could not afford to have their enterprise closed or destroyed.

An interesting addition to this issue set is the illegal or quasi-legal franchising of cyber crime. Criminals now market and sell the tools of cyber crime. Root kits, hacking lessons, guides to designing malware—it is all available. These range from rudimentary "starter kits" to highly sophisticated programs that are potentially very destructive.

The last and, in my mind, most interesting and insidious threat is the rise of the botnets. Criminals cannot command entire nations of computers as one would expect that coercive governments could if they need to. Criminal syndicates have, however, developed huge botnets with members all over the world: members that they control without the actual owner of the machine even being aware of it. These zombie networks serve their criminal masters without question or hesitation. The criminals control them completely and can use them directly for DDoS (distributed denial of service) attacks, phishing, or malware distribution. They also rent them out to others for cash.

An anecdote will illustrate how pervasive this is. During an industry association meeting held in December of 2008, a U.S. Department of Homeland Security (DHS) official involved in cyber security

related an incident that had occurred a few days prior. He said he had been meeting with a group of business leaders, and they expressed concern about a holiday season trend they had noticed. They complained that every year many young people received new computers as gifts, causing a big spike in computer intrusions. They blamed this on the young people using the new devices to try and hack government and business systems.

The DHS official explained to the leaders that they were only half right. He went on to explain that the many new machines were connected to the spike in intrusions—however, not because their owners were all would-be hackers. The problem lay in the fact that in some cases, within 10 to 15 minutes of a new computer being hooked to the Internet, it was infected by malware and added to a criminal botnet. The longest an unprotected or underprotected computer would last was a day or two. It was criminal-controlled botnets that were behind the spike in intrusions. They simply had many new machines to utilize in their activities.

It is here that a new and very dangerous potential arises.

## Terrorism Enabled by Cyber Criminals: Most Likely Cyber Threat

There is no doubt that terrorists want badly to hurt the modern Western and Western-leaning community of nations. The numerous dead and wounded, the horrific damage of past successful attacks, as well as the multiple foiled plots all make the deadly intent of the terrorists abundantly clear to all. This cannot be denied. Their continuing efforts to acquire and develop weapons of mass destruction for use against civilian targets is also *prima facie* evidence of this burning desire to do us harm in any way possible.

Terrorist organizations surely can find a number of highly trained, intelligent, and computer-literate people who are in agreement with their cause. These people can be taught to develop code, write malware, and hack as well as anyone. They cannot, in a timely manner, develop the kind of large-scale operational capabilities that a nation-state possesses. This is what they need to make a truly effective assault on the West in the cyber realm.

Two factors give them another option. First, they do not really need to attack an entire nation to achieve success. They desire to create a large event, but it does not necessarily need to be as extensive as a full nation-state attack. The second factor is that they also have abundant funds and potential access to even more. These funds open up the criminal option, which will give the terrorists the capability to be extraordinarily destructive.

The West has a huge number of intelligence and law enforcement assets dedicated to stopping the proliferation of weapons of mass destruction. Any movement of these devices or materials related to them will sound the alarm across the world. Numerous arrests of people attempting to traffic in WMD or related materials have been made. This effort has nullified the effect of the excellent financial assets some terrorists have and frustrated their efforts to acquire WMD capabilities. We do not have the same type of watchdog systems in place to prevent cyber enablement from occurring.

If a cash-rich terrorist group would use its wealth to hire cyber criminal botnets for their own use, we would have a major problem. A terrorist group so enabled could begin to overwhelm the cyber defenses of a specific corporation, government organization, or infrastructure sector and do much damage. They could destroy or corrupt vital data in the financial sector, cripple communications over a wide area to spread panic and uncertainty.

Similar to the nation-state attack scenarios discussed earlier, terrorists could use botnet-driven DDoS attacks to blind security forces at a border crossing point as a means of facilitating an infiltration operation, or a cyber attack in one area of a country to act as a diversion so a "conventional" kinetic terrorist attack can occur elsewhere. They could even conduct SCADA attacks on specific sites and use the system to create kinetic-like effects without the kinetic component. A good example would be to open the valves at a chemical plant near a population center, creating a Bhopal-like event.

The permutations are as endless as one's imagination. The cyber capabilities that the criminals could provide would in short order make any terrorist organization infinitely more dangerous and effective.

Some have opined that cyber attacks are not suitable as terror tactics because they lack the drama and spectacular effect of, say, a suicide bomber. This does not take into account the ability of the terrorists to adapt. As our intelligence and law enforcement agencies continue to effectively combat the terrorists, they will continue to evolve. The terrorists' old methods will be augmented and improved. They will need to develop more imagination and versatility if they are to conduct successful operations.

This evolutionary capability has not been in short supply among the terrorist leadership. They will not define "spectacular" so narrowly. Imagine the operational elegance of simply hitting the return key and seeing thousands of enemies die a continent away, or watching a bank go under due to the destruction of all its data by an unknown force. This will be enormously attractive to terrorist groups. Additionally, the combination of cyber methods and kinetic strikes could be spectacular regardless of one's definition.

Criminals, for their part, are motivated by greed and power. Few of the leaders of the enormous cyber organized crime world would hesitate at selling their capabilities to a terrorist loaded with cash. That fact, combined with the ever-growing terrorist awareness of cyber vulnerabilities, makes this set of scenarios not just likely, but *nearly inevitable*.

## Conclusion

Terrorists will recognize the opportunity the cyber world offers sooner or later. They will also recognize that they need help to properly exploit it. It is unlikely they will have the patience to develop their own completely independent capabilities. At the same time, the highly developed, highly capable cyber criminal networks want money and care little about the source.

This is a marriage made in Hell. The threat of a full nation-state attack, either cyber or cyber-enabled kinetic, is our most dangerous threat. We pray deterrence will continue to hold, and we should take all measures to shore up that deterrence.

Terrorists will never be deterred in this way. They will continue to seek ways to successfully harm us, and they will join hands with criminal elements to do so. A terrorist attack enabled by cyber crime capabilities will now be an eighth group of cyber threats, and it will be the most likely major event we will need to confront.

Some would say that cyber crime is a purely law enforcement issue, with no national security component. That is a dubious "truth" today. This is not a static situation, and it will definitely be more dangerously false in the future. Unless we get cyber crime under control, it will mutate into a very real, very dangerous national security issue with potentially catastrophic ramifications. It would be far better to address it now rather than in the midst of a terrorist incident or campaign of incidents against one of our countries.

Terrorism enabled by cyber criminals is our most likely major cyber threat. It must be met with all our assets.

*—Dr. Steven P. Bucci is IBM's Issue Lead for Cyber Security Programs and a part of the Global Leadership Initiative, the in-house think tank for IBM's public-sector practice. He most recently served as Deputy Assistant Secretary of Defense, Homeland Defense and Defense Support to Civil Authorities. Dr. Bucci delivered these remarks at a meeting of The Heritage Foundation's Cyber Security Working Group. The views expressed are his own and do not necessarily reflect the institutional position or views of IBM, its board of directors, or any of its subsidiaries.*