IF 2919
September 2, 2008

A WILDERNESS OF MIRRORS: THE INTERNET BECOMES A LIABILITY

Cyber-invasions of Estonia in 2007 and Georgia this summer have altered the perception of the Internet as an always-positive economic force. Escalating levels of sophistication in cyber-crime are altering the same perceptions for businesses. New techniques and new capabilities have elevated the cyber-criminal's and the cyber-warrior's ability to wreak damage on selected targets.

With this new escalation has come a bigger enforcement problem: how to identify and locate those who launch attacks. "Botnets" enable their criminal or military operators to commandeer computers anywhere in the world – without their owners' knowledge, making the attacks seem to come from everywhere confusing those who might want to respond to the origins of the problem.

This new cyber-reality has several characteristics: (1) Assaults come from everywhere, at any time; (2) they're easy and cheap; and (3) flexibility and confusion rule. Now that individuals, criminal gangs and militaries can launch massive cyber-attacks from computers based anywhere in the world, effective security, enforcement and response to the attacks are going to get more complex, potentially making the Internet a major liability as well as an asset.

Planetary Emergencies

Theoretical physicist Dr. Antonino Zichichi hosted his fortieth annual conference on "Planetary Emergencies," an assemblage of world-renowned scientists, engineers, economists and analysts who gather yearly in Erice (Italy) to identify and exchange data on the most pressing problems facing the globe. This year's conference focused on energy shortages, nuclear weapons, climate change and **cyber-war**. Discussion on this last topic included a look at "bot herders," computer hackers who capture and deploy

millions of computers around the world and put that digitally lethal combination at the disposal of any cause, anywhere, so long as that cause is backed by money to pay the cyber-mercenaries what they demand. (*New York Times*, 8/24/08)

"Interesting business proposal. We'll have to run it by illegal."

The scientists who gathered in mid-August would not have needed to travel very far afield to witness cyber-war in practice. Weeks before Georgia's troops crossed into South Ossetia to quell separatist fervor there and Russia's troops crossed into South Ossetia and other parts of Georgia, someone somewhere unleashed a withering attack on Georgia's state-owned and commercial Internet sites, essentially shuttering the state's Internet infrastructure as well as the country's private media, communications and transportation control systems. (*New York Times*, 8/13/08)

The attacks started on July 20, when Georgian Web sites received a barrage of requests for information, so many requests that the sites became unable to function – a so-called distributed denial of service (DDOS) attack. After hours of trying to uncover what was taking place, Georgian officials finally blocked the attacking computers' access, which meant blocking access from the United States where most of the attacking computers and servers were located. But those managing the attacks simply shifted their operations to a server owned by a Russian communications company in Moscow, whose owners might not have known that their system was being used. And so, the DDOS assault on Georgia resumed. The initial DDOS attack was followed by another level of "invasion," which redirected Georgian Internet traffic through Russian telecommunications sites, where it could be dropped or forwarded incorrectly. Then Georgian troops crossed into South Ossetia and Abkhazia on August 7, and then Russian troops entered South Ossetia on August 10. The July 20 digital attack was the first cyber-assault ever to accompany or precede an actual military shooting war, which, in this instance, started August 10. (*International Herald Tribune*, 8/13/08)

What is particularly curious about the Russian invasion of South Ossetia and Abkhazia is the fact that the cyber-assault that preceded that incursion had already started weeks before Georgia sent its troops to South Ossetia to bring the breakaway province back to central government control. Evidently, Georgia's President Mikhail Saakashvili had planned his military deployment into South Ossetia for a date near August 8 when Russia's Prime Minister Vladimir Putin would be in Beijing for the Olympics' opening ceremony. But given that the cyber-attack had by that time already shut down Saakashvili's own Web site, he should have sensed that all would not be proceeding as he had planned. Perhaps he did not take cyber-warfare seriously enough. (*Guardian Weekly*, 8/15/08)

"Nope. That's not one of the stories I'm working on."

Jaak Aaviksoo, Estonia's defense minister, takes cyber-war very seriously. His country suffered a blistering cyber-attack last spring. When hackers and cyber-warriors invaded Georgia, the damage to critical infrastructure was limited by the fact that Georgia ranks only seventy-fourth among nations in deployment of Internet connections – that is, its Internet systems are less developed than even those in Nigeria and Bangladesh. Estonia, on the other hand, is one of the most "wired" countries in the world, and the digital assault it suffered in May 2007 disabled critical resources, including government operations and electricity networks. (*New York Times*, 8/13/08)

The Estonian attack came in three waves. First came the "script kiddies," a mass of individual computer hackers who had downloaded a simple program from online sources, enabling them to participate in a massive – even if uncoordinated – DDOS assault that clogged and choked Internet-based systems at Estonian newspapers, television stations, schools and eventually banks. Web sites operated by these private Estonian companies normally received **1,000 visits per day**, but suddenly they were overwhelmed by requests for information arriving at a pace of **2,000 per second**. Then came the "botnet" ("ro**bot net**work") onslaught: more than one million "zombie" or captured computers situated in 70 countries, assembled by cyber-warriors who had distributed a computer virus that made the infected computers respond to the commands of the botnet's operators, without the computers' owners even knowing. This made the attack seem to come from everywhere. And finally, the attackers let loose their "special forces," individual hackers who "invaded" specific Web sites and disabled critical resources. This third wave of the organized attack included a "Trojan horse" virus that took control of computers inside Estonia and then assembled them together into a domestic botnet. As a result, when officials in the capital, Tallinn, closed off the country's international link to the Internet to halt the attack, the residual compromised computers continued to do harm internally. (*Wired*, 8/21/07; *International Herald Tribune*, 5/18/07; *Georgetown Journal of International Affairs*, Winter/08)

After the Estonia attack ended, NATO's official spokesman noted ominously – and as it turned out, correctly: "Today Estonia, tomorrow it could be somebody else." Yet from a military point of view, confusion over who actually launched the attack made an effective response difficult. With computers participating in the attack sitting in 70 different countries, the question, as phrased by General William T. Lord, head of the U.S. Air Force's Cyber Command, became: "Who do you take action against?" (*Popular Mechanics*, 9/08)

Who's Attacking Us?

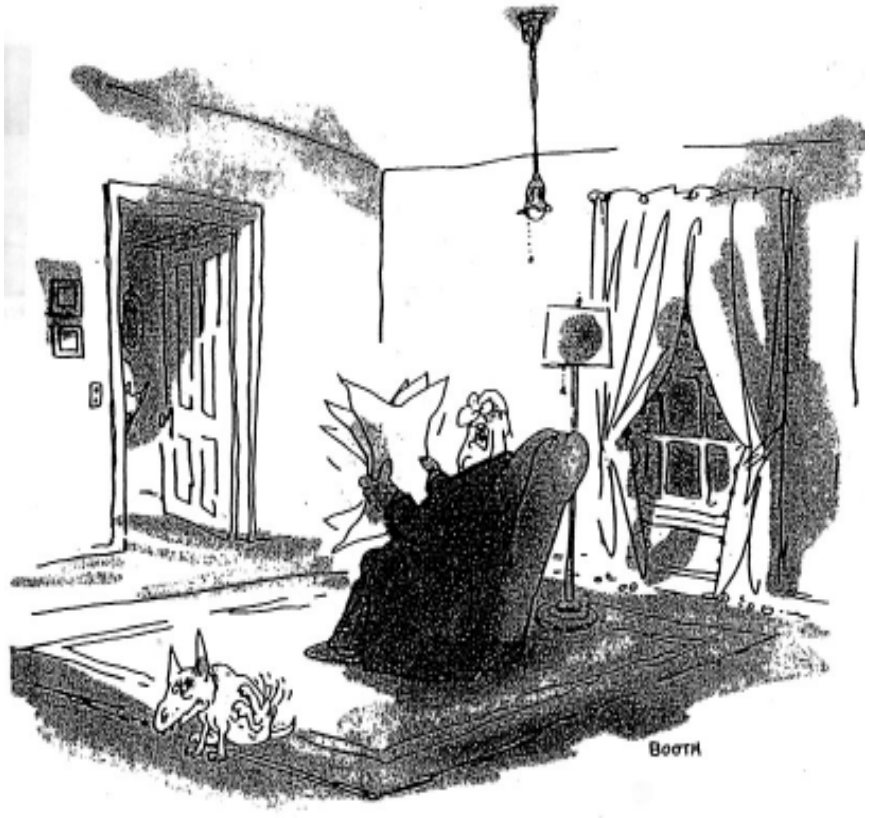
When Estonia suffered its attack, even though zombie computers were in 70 different countries, the vast majority of the compromised computers were located in Egypt, Vietnam and Peru, countries that hardly had political issues with Estonia. When cyber-warriors hit Georgia, the majority of participating computers were in the U.S., an ally of Georgia. Because of the anonymity of global botnets, it can be nearly impossible to determine who controls the robot network of computers and who is "invading" the targeted country.

"Special Forces."

As noted by one Israeli network security specialist who was helping Georgia mount a response, "The nature of what's going on isn't clear." (*New York Times*, 8/13/08)

This is where the assessment of the Planetary Emergencies conference becomes intriguing. Scientists there did not focus just on cyber-war or digital terrorism. Rather, they worried about "bot herders," massive networks of zombie computers controlled by hackers who rent their networks and talents for a price. Computer security specialists assessing what had taken place in Georgia concluded that the particular way the DDOS attack took place bore the operational imprint of a Russian criminal gang known as the Russian Business Network (RBN). Even that, however, is not certain. Yet the idea that these kinds of hacker groups exist for hire adds a mercenary overlay to the already confusing situation. Such a mercenary enterprise gives the hiring country deniability and misleads those trying to decipher what is taking place. As a result, launching a cyber-attack no longer requires technological capabilities – only the money needed to pay for the operation. Interesting enough, a recent study revealed that the cost of each compromised computer in a botnet raid is just four cents, putting such clandestine criminal attacks within reach of many mischievous individuals and organizations, let alone countries. Or, as Bill Woodcock who tracks Internet traffic for Packet Clearing House explained in more colorful language, "You could fund an entire cyber-war for the cost of a tank tread." (*New York Times*, 8/13/08; *New Scientist*, 8/23/08)

The confusion that results from not knowing "Who is doing what to whom, for whom, with what and from where" goes beyond typical wartime dislocation – often called the fog of war. Uncovering who is behind an attack, as one analyst noted, is like untangling "a web of lies." As a result, some in the security field are borrowing a metaphor from the tangled and deceptive world of global espionage to characterize the situation surrounding the new cyber-war: "a wilderness of mirrors."



"I'd just like to know what in hell is happening, that's all! I'd like to know what in hell is happening! Do <u>you</u> know what in hell is happening?"

It's Not Just War

The military capability to evade discovery, move resources quickly and access needed information has commercial – or more precisely criminal – value as well. In another instance from earlier this year, a criminal gang – allegedly based in Russia as well – successfully infected 378,000 computers over 16 months, a process that enabled the gang to acquire valuable information to be later used in fraudulent practices. The gang sent digital viruses through the Internet to "infect" computers with a program called Coreflood, which would then record the computer user's keystrokes, enabling the gang to capture screen data, passwords and other

information, which they used to access accounts. More critically, when the gang captured the machine of a system administrator, it exploited a Microsoft tool that enabled the administrator computer to update all the computers under it at once. The gang used that tool to send "Trojan horse" software to all the computers associated with the captured administrator computer, thereby reaching the administrator's entire network with one keystroke. (*New York Times*, 8/6/08)

Malicious attacks on computers at the U.S. Department of Defense increased by 31 percent from 2006 to 2007. But that increase pales in comparison to the upturn in malicious activity in general. A few years ago, computer security analysts were identifying roughly 5,000 new viruses **each year**. Currently, they are seeing 15,000 new viruses **each week**. (*Popular Mechanics*, 9/08; *Newsweek*, 8/11/08)

Not all Internet vulnerabilities for commercial enterprises involve sophisticated hacking systems. For instance, the U.S. Justice Department just charged 11 individuals in connection with a hacking operation that stole nearly 41 million credit- and debit-card numbers from at least nine major retailers, including TJX (owner of TJ Maxx, Marshalls, Home Goods and AJ Wright). As if to verify the confusion surrounding such thievery, officials revealed that 8 of the 11 were still at large and that one of them was still known only by his online alias. (*Dallas Morning News*, 8/6/08)

These thieves preferred "war driving," the simple act of driving their cars near retail outlets, pulling out laptop computers and checking to see if any store had an accessible wireless network. When they found one, they installed "sniffer programs" that would capture card data through the retailer's processing networks. That is, they did not enter the company's database but instead actually monitored and captured data being transferred during sales transactions, a segment of the retail data network heretofore thought to be especially secure. For safe keeping, the thieves stored the purloined data on servers in Latvia and the Ukraine. (*Dallas Morning News*, 8/6/08)

An even more ominous reality recently came to light. The domain name system (DNS) converts common-language Web site names into Internet friendly numeric names. In July, the United States Computer Emergency Readiness Team (U.S.-CERT), the government's cyber-security arm, reported the discovery of a flaw in the DNS operation that would allow a criminal to alter the numeric translation and divert computer users to fake Web sites, even when users type the correct address into the system. For instance, Web surfers could type InferentialFocus.com correctly on their Web search browser, but using the flaw in DNS, a hacker could redirect that user to a bogus Web site that looks and feels like the Inferential Focus Web site. Once the innocent user is on the fake site, the hacker can request or capture critical information about the user. In the instance of financial institutions' Web sites, the hacker could steal critical passwords and account data. (*International Herald Tribune*, 7/31/08)

For that reason and because of the seriousness of this vulnerability, officials postponed for months public notification of the flaw to give Microsoft, Cisco, Sun and the other 80 or so affected software vendors time to write fixes for the flaw. Given that no central entity operates the Internet, no single authority exists to protect the millions of vulnerable computers. As a result, individuals and institutions will need to apply the software patches on their own, and do so before hackers exploit the vulnerability. (*Information Week*, 7/14/08)

"Something bad's happened. The third caller to guess what it is will win dinner for two at Romeo's Italian Garden."

A Digital World

In our 2007 looks at the increasing risks of cyber-attacks, we noted that as many as 11 million computers were, at that time, controlled by a botnet hacker, all without the knowledge of those computers' owners. We also noted that beyond the geopolitical and commercial hacking for military or criminal purposes, botnets were also responsible for 80 percent of the spam sent through the Internet (see **eFocus 201**, 2/16/07 and **eFocus 210**, 8/31/07).

When that is matched with the recent increase in the number and severity of hacker attacks on secured and unsecured systems, the sense that something has changed in the cyber-world starts to emerge. Our observations suggest that a new Internet vulnerability is developing, and it is creating a different world for those who depend on the Internet for communications, operations and data storage. Here are a few of the attributes of this new cyber-vulnerability.

Assaults come from everywhere, at any time – The fact that security personnel confront roughly 15,000 new computer viruses each week means that security breaches are likely at any time, anywhere. Breaking through the Microsoft administrator tool, hackers can compromise an entire network of computers at once, and the vulnerability of the domain-name system, should it not get protected, puts online enterprises at risk to no longer assure their customers a secure point of access. (*Newsweek*, 8/11/08)

They're easy and cheap – "War driving," the practice of using a laptop to look for accessible wireless systems, is quite easy to do, as is the "script kiddy" approach to sending distributed denial of service assaults. Anyone can park a car in front of a retail outlet and test for an Internet access point, and anyone can download a simple program and activate it to send unwanted messages to target computers. As noted earlier, botnets cost only 4 cents per captured computer. (*International Herald Tribune*, 8/13/08)

Flexibility and confusion rule – When the Georgian attacks were discovered to be centered on servers based in the U.S., security people closed that access point, but the hackers quickly shifted their server location to Russia. When U.S. authorities traced a criminal gang's server to Wisconsin, the cyber-thieves quickly relocated it to the Ukraine. Moreover, where they placed their servers had nothing to do with where the perpetrators were – thus the confusion over identifying and locating those responsible for an attack or a crime. No one knows yet who actually launched either the Estonian or the Georgian attacks; no one even knows who started a much simpler and less malicious 2001 attack on the U.S. White House Web sites – dubbed at the time the Red Alert attack. (*Scientific American*, 9/07; *Georgetown Journal of International Affairs*, Winter/08)

"Let's change 'brink of chaos' to 'Everything is wonderful.'"

Confusion and uncertainty are effects of what we have called World War III – the Battle over Permeable Borders. Whether in the areas of science, technology, business, geopolitics, nature or personal life, someone is trying to knock down a barrier, boundary or border that was once was accepted as real. Meanwhile, someone else wants to resurrect, support or strengthen that same barrier, boundary or border – thus the battle lines of

World War III are drawn. As a result, confusion and uncertainty abound in societies around the world – what can be counted on anymore? (see "Living with World War III, Part I: Permeable Borders, Uncertainty and Instability," **IF 2311**, 5/1/02).

The cyber-war situation adds to that confusion, with potentially strategic and expensive consequences. "If you have a missile attack against, let's say, an airport, it is an act of war," explains Madis Mikko of the Estonian Defense Ministry. "If the same result is caused by computers, then how else do you describe that kind of an attack?" Ene Ergma, speaker of the Estonian parliament, adds to the battle metaphor with a bit more emphasis: "When I look at a nuclear explosion and the explosion that happened in our country in May [2007], I see the same thing. Like nuclear radiation, cyber-war doesn't make you bleed, but it can destroy everything." (*International Herald Tribune*, 5/18/07; *Wired*, 8/21/07)

The Estonians think NATO should have come to their defense with military force, but as General Lord noted, "Who do you take action against?" If specialists cannot be sure who triggered a given cyber-battle, how can a country respond appropriately? Moreover, if the cyber-warriors are mercenaries – hired criminals with cyber-expertise and with no single national identity – the task of recognizing the political entities linked to the attacks becomes even more complex.

Yet cyber risks do exist and are increasing. That is why the U.S. military now has several different special cyber-war units working on defense strategies. Evidently, an equal sense of urgency to halt the advance of botnets and mass cyber-attacks has not yet reached some corporate boardrooms. "The rate of [computer] infection is still high," observed one security consultant, "but concern among corporations is low. Many corporations seem to think it's O.K. to be infected several times a month." (*New York Times*, 8/6/08)

The Identity Theft Resource Center, a nonprofit U.S. organization dedicated to preventing identity thefts, recently reported that officially 22 million consumer files at 449 different businesses have been compromised so far this year. But the group added that just 41 percent of companies reporting such an invasion included figures about the number of consumer files compromised. Moreover, the group noted that an untold number of corporations have chosen not to reveal when they have been invaded, let alone share the number of consumer files compromised. Whether or not companies wish to make their internal breaches public, the costs can be heavy. In the instance of the TJX file theft, which was made by war-driving hackers, lawsuits and other expenses eventually cost the company several hundred million dollars. (*Atlanta Journal-Constitution*, 8/27/08)

Hamadoun Touré, secretary-general of the International Telecommunication Union, speaking at the August Planetary Emergencies conference in Italy noted that computers and the Internet offer the prospect of creating a global "knowledge society," but that such a society comes with attendant risks. "Every single brain on earth is equal," he told the assembled scientists and analysts, "and [each] can trigger an attack." (*New York Times*, 8/24/08)

When every "brain" everywhere can launch a military or criminal attack and count on the "wilderness of mirrors" to remain undetected, society has clearly entered a different era of warfare and crime. The Internet, which has been praised in so many ways for its assets, is becoming a noteworthy liability for governments, corporations and individuals.