CBRNF – A new addition (F=Financial)?

CBRNE Newsletter Terrorism

Volume 48, 2013

Cyber News

The Few and The Brave!

www.cbrne-terrorism-newsletter.com

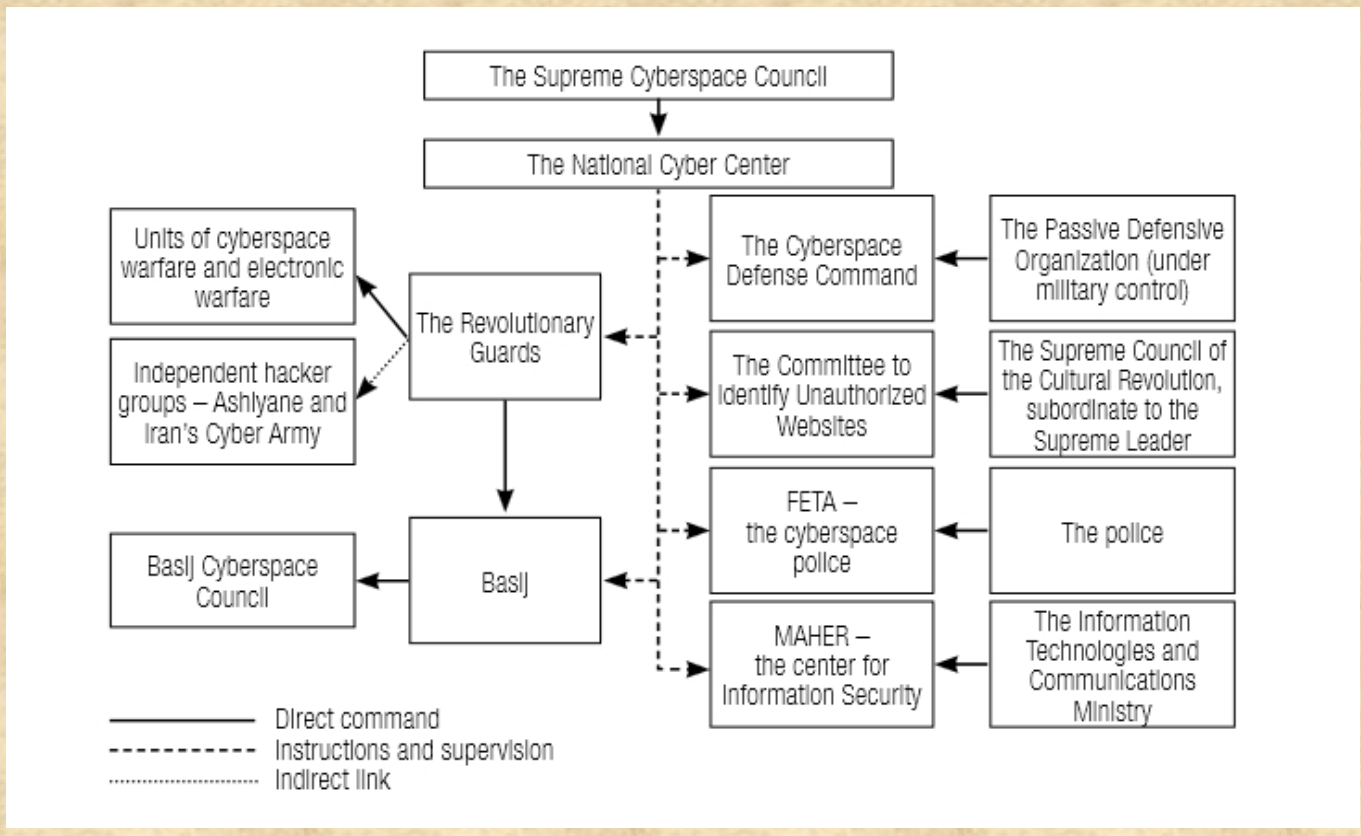
Iran and Cyberspace Warfare

By Siboni, Gabi and Kronenfeld, Sami

Source: http://www.inss.org.il/research.php?cat=524&incat=&read=11055

Since the Stuxnet attack – one of the most destructive cyber attacks to date – Iran has been working hard to improve its cyberspace defenses on the one hand, while building up cyberspace intelligence gathering and offensive capabilities on the other.

The Iranian cyberspace defense program has a dual objective: first, it hopes to prevent another attack like Stuxnet and intelligence-directed penetration of Iranian computers by viruses such as Duqu and Flame. In this sense, the goal of the Iranian program is similar to that of many other nations seeking to protect their critical infrastructures. The second objective is the regime's desire to ensure its survival by means of surveillance and blocking of information and services originating with the Iranian public. In



many cases the two goals are achieved with the same tools, e.g., the Iranian effort to create a separate Iranian web or the disabling of Google services in that country.

This article examines the current situation regarding various elements of Iran's cyberspace development process. The first section analyzes the country's cyberspace strategy, while the second section describes the organizational and operational response to the formulated strategy. This comprises three components: infrastructures for training and developing technological manpower for work in cyberspace; technological developments that have already been introduced; and the overall processes of cyberspace force construction. Finally, the article focuses on a number of cyberspace incidents attributed to Iran, attempts to gain some insight into the way Iran conducts its cyberspace activities, and examines implications for Israel and other Western nations.

► **Read full paper at:**
http://cdn.www.inss.org.il.reblazecdn.net/upload/%28FILE%291362314938.pdf

Chinese government orchestrates cyberattacks on U.S.: experts

Source: http://www.homelandsecuritynewswire.com/dr20130219-chinese-government-orchestrates-cyberattacks-on-u-s-experts

For more than a decade now, China has engaged in a sustained, systemic, and comprehensive campaign of cyber attacks against the United States. The Chinese government has enlisted China's sprawling military and civilian intelligence services, with their armies of cyber-specialists, in a cyber-campaign aiming to achieve three goals: steal Western industrial secrets and give them to Chinese companies, so these companies could compete and weaken their Western rivals; hasten China's march toward regional, then global, economic hegemony; achieve deep penetration of U.S. critical infrastructure in order to gain the ability to disrupt and manipulate American critical infrastructure – and paralyze it during times of crisis and conflict. A detailed 60-page study, to be released today , offers, for the first time, proof that the most sophisticated Chinese hacker groups, groups conducting the most threatening attacks on the United States, are affiliated with the headquarters of China's military intelligence lead unit — PLA Unit 61398.

- The immediate goal is to steal the engineering and industrial secrets developed by American scientists and engineers working for American corporations, and give these secrets to Chinese companies. These companies, in many cases owned by or affiliated with the Peoples' Liberation Army (PLA), then turn around and compete with the very companies whose secrets the Chinese intelligence services had stolen. The Chinese companies more often than not succeed in stealing business away from Western companies because the Chinese products offer the same benefits the products of the Western companies do (these Chinese products, after all, are based on technologies stolen from Western technology) – but are cheaper, because often these Chinese companies are subsidized, directly or indirectly, by the Chinese government.
- China's intermediate goal is to erode the U.S. economic advantage over China, and

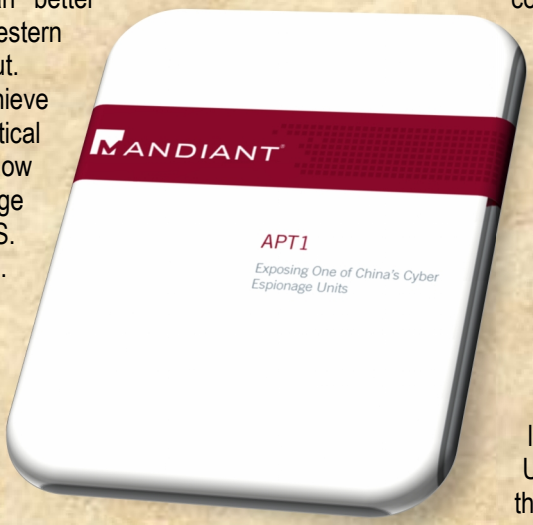
achieve regional, then global, economic hegemony. China is taking several other steps to hasten its march toward hegemony – it invests billions of dollars in improving its own science education and research, builds up its military, and flexes its muscles in an effort to intimidate its regional rivals. These measures take time, however. Stealing Western industrial secrets, and then using the stolen technologies to strengthen Chinese companies so they can better compete against and weaken Western companies, is an attractive short-cut.

- China's longer-term goal is to achieve deep penetration of U.S. critical infrastructure which would allow China to do two things: first, engage in subtle disruptions of, say, U.S. financial institutions or the U.S. power generation and distribution system in order to create confusion, difficulties, and mayhem in the United States during times of U.S.-Chinese tensions. The second goal is to gain the ability to paralyze the United States outright during times of crisis and open conflict by shutting down U.S. critical infrastructure – or taking control of it. Thus, Chinese sleeper malware may be activated to turn off power generation stations and plunge cities into darkness, or remotely open dam gates to release reservoir water and cause massive floods.

The *New York Time* reports that a detailed 60-page study, to be released today by U.S. computer-security firm Tuesday by Mandian, offers, for the first time, proof that individual hackers belonging to the most sophisticated Chinese hacking groups — known in the United States as "Comment Crew" or "Shanghai Group" — are affiliated with the headquarters of PLA Unit 61398.

"Either they are coming from inside Unit 61398," Kevin Mandia, the founder and chief executive of Mandiant, told the *Times* last week, "or the people who run the most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood."

The *Times* notes that other security firms tracking Comment Crew have concluded the group is state-sponsored. A recent classified National Intelligence Estimate (NIE), representing the views if all U.S. sixteen intelligence agencies, asserts that many of these hacking groups are either run by army officers or are contractors working for commands like Unit 61398.



The *Times* notes that for U.S. intelligence and security agencies, the most worrisome aspect of the latest series of attacks launched by Unit 61398, is that these attacks focus not merely on stealing information, but on gaining the ability to disrupt and manipulate American critical infrastructure.

One recent example is the successful Chinese hacking of the Canadian arm of Telvent. The company, now owned by Schneider Electric, designs software that gives oil and gas pipeline companies and power grid operators remote access to valves, switches, and security systems.

In his State of the Union address, president Barack Obama gave expression to this growing U.S. concern about the scope, sophistication, and goals of China's cyber warfare campaign against the United States. Without mentioning China by name, Obama said: "We know foreign countries and companies swipe our corporate secrets…. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems. We cannot look back years from now and wonder why we did nothing."

Read the Mandiant Report at: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

America's Top Cyberwarrior Says Cyberattacks Cost $250 Billion A Year

Source: http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559

The U.S.'s leading cyberwarrior says companies are losing hundreds of billions to cyberespionage and cybercrimes, and spending even more trying to prevent them.

But whether there is any cohesive strategy to tackle the problem, and whether the government even has a larger role to play, remains up for debate.

Four-star Gen. Keith Alexander, director of the supersecret National Security Agency and head of the Pentagon's Cyber Command, said the illicit cyberspace activities essentially amounted to the greatest transfer of wealth in history. Alexander warned Congress earlier this year about the dangers to national security from cyber threats.

Speaking Monday to an audience of scholars and industry experts at the American Enterprise Institute, a conservative-leaning Washington think tank, Alexander said U.S. companies lose some $250 billion to intellectual property theft every year, citing figures from Symantec, a leading security software maker. Internationally, $114 billion was lost to cybercrimes, but that number could be as high as $388 billion if the value of time and business opportunities lost is included. McAfee, the computer software and security company, gives an even higher number, saying $1 trillion is spent globally in remediation efforts.

Alexander said 2011 and early 2012 in particular has been a rough time in the fight for cyberspace. But government and companies appear to have been fighting a losing battle for three years now.

McAfee has now identified some 75 million unique pieces of malware in its databases. Botnets send out 89.5 billion pieces of spam email each day, almost a third of all emails that move through the Internet. In 2009, there were only nine cyberattacks on U.S. critical infrastructure; in 2011 there were more than 160.

No surprise then, that analysts in intelligence, business, and technologies call it one of the major challenges of the current information

age. President Barack Obama called cyberthreats one of the most serious economic and national security challenges we face, in 2009.

In 2011, the number of cyberattacks increased 44 percent over the previous year, and the amount of malware on the Internet jumped some 60 percent.

Over the past year, numerous leading international and American companies have been successfully targeted by cyberattacks. Google, Booz Allen, Mitsubishi Heavy Industries, Sony, and AT&T were respectively hacked in June, August, September, October and November of 2011. Symantec itself was attacked in January 2012. In April, Nissan, Visa, and MasterCard were hacked.

That list only begins to describe some of the massive challenges facing companies today in digital self-protection. Rodney Joffe, a senior technologist at Neustar Inc. who advises the White House, told Reuters in June that of 168 companies he surveyed from the Fortune 500, 162 had been hacked in the recent past. The FBI estimates that for every company that is aware it has been hacked, 100 others don't know they have been attacked.

Alexander urged the U.S. to take a larger leading role in the current fight against cybercrime. Since America originated much of the technology being used to increase the world's connectivity, we have to be the ones to secure it, said the general.

But who specifically -- government or businesses -- would be doing that securing remains in dispute.

Experts hosted by AEI responded to Alexander's speech by pinpointing U.S. opponents in cyberspace and discussing means to tackle the problem. Michelle Van Cleave of the Homeland Security Policy Institute implicated China's cyberespionage efforts as the biggest threat to U.S. companies and law enforcement, calling the current approach to dealing with such attacks inadequate. Van Cleave reflects a growing voice in U.S. government which seeks to pressure China in particular, seeing it as the leading cyber-antagonist of the U.S.

Yet others have been cautioning against exclusively targeting China, or giving more responsibility to the U.S. government.

Adam Segal, an expert on security issues at the Council on Foreign Relations, said there was no reason to doubt China's claims that highly capable U.S. agencies like the NSA may already have deep access to Chinese government and military systems -- when the U.S. usually claims it is the other way around. Segal said the Chinese government feels victimized by the U.S., which it sees as having a major cyberspace advantage. Reliance on foreign technologies and U.S. companies like Cisco and Oracle, coupled with a new American military presence in cyberspace like the Cyber Command led by Alexander, has fostered a sense of insecurity in China.

Jeff Snyder, vice president of Raytheon, noted that America faces diverse challenges apart from state-based actors, including disgruntled employees and infiltrators foreign and domestic.

Indeed, the nature of cyberattacks means that belligerent parties are almost always difficult to trace. Alexander noted the dynamic created a fundamentally different problem from nuclear deterrent strategies of the past.

Jim Harper, the director of information policy studies at the Cato Institute, a libertarian Washington think tank, was wary of the move to hand over responsibilities for protecting private companies, especially large and wealthy private companies, to the government. Harper argued that corporations themselves have a duty to be responsible for their own security, and a liability should they fail to protect their networks. Asking the government to take on additional burdens would only increase costs to the public.

Harper believes the public does not have an inherent interest to protect the intellectual property of private parties, only to provide the means for those parties to protect themselves.

Experts largely agree that it would take at least another decade, if not longer, to create any kind of meaningful international consensus on cybersecurity norms.

In the meantime, at least according to Alexander, the threat is getting worse. He warned that while the nature of attacks today still remained largely disruptive, trends indicate that they are transitioning to becoming destructive. In other words, cyberattackers are moving not only to block communications between computers, but will soon become capable of destroying computers and the physical infrastructure they control as well.

Other countries, particularly those suspected of being the most active

cyberattackers by the U.S., are not expected to cooperate easily. After all, they have plenty of reason to suspect that Pandora's box of destructive cyberattacks may have been opened by the U.S. itself. Analysts strongly consider cyberattacks carried out against Iran in 2010 and 2012 to hinder its nuclear program through computer worms Stuxnet and Flame to have been launched by Israel, likely with U.S. assistance.

In addition, the reliance of U.S. companies, government and military on digital communications makes cyberattacks an especially effective asymmetric weapon of choice for individuals and groups in places like Russia, China, and Iran.

But the future is not all that gloomy, even for those working to avert worst-case scenarios.

Alexander himself noted the astronomical changes and improvements the current information age had already made to people's lives.

In 2000, the Internet population only numbered 360 million; by the first quarter of 2012, it was already 2.3 billion strong. Around the world, 461 million mobile phones were sold in 2011, and there could be more active cell phones than human beings on the planet within the next four years. The power of social networks is also increasing. Facebook is expected to have 1 billion user accounts by August 2012, not all of which are unique, but enough to make it the third-largest country in the world, if accounts translated to population.

Think about all the opportunities that we have, said Alexander, discussing the benefits new communications and computing would have on the future of medicine, education, and scientific growth

.

Cyberspace and Terrorist Organizations

By Yoram Schweitzer, Gabi Siboni, and Einav Yogev

Source:http://i-hls.com/wp-content/uploads/2013/03/Cyberspace-and-Terrorist-Organizations.pdf?330fa1&utm_source=Terrorism+in+CyberSpace&utm_campaign=ACD%2FEWI+BLOG&utm_medium=email

At first it would seem that the movie is nothing but another Hollywood fantasy, dismissible as a wild exaggeration carriedto yet further extremes in the sequel, Die Hard 4. However, the events of 9/11 and the changes in the nature of security threats over the last decade indicate that even the most far-fetched scenarios crafted in Hollywood studios are liable to find real-life expression in the public and security sphere in this day and age.

The use of cyberspace as a primary warfare arena between enemies or hostile nations has always been fertile ground for fantasy and lurid scenes on the silver screen. However, cyberspace is rapidly becoming a genuine central arena for future wars and hostile actions undertaken by various types of adversaries. These may include terrorist organizations, although until now they have relied primarily on physical violence to promote their own goals and those of their sponsors. In light of such threats, many nations in the West have in recent years established special authorities to use innovative technological means to prepare for war-like actions against strategic infrastructure targets.

The Cyber Threat from Terrorist Groups

Today there are five main groups that use or have the potential for future use of cyber-attack tools:

1) **states** developing offensive and defensive capabilities as a growing part of their force capabilities;

2) **criminal** elements motivated primarily by illegal commercial interests;

3) **commercial** companies, primarily in the defensive mode (as the scope of cyber-attacks in the commercial context is significantly growing), though some may resort to offensive moves against competitors;

4) **terrorist** organizations, out of cost-benefit considerations and other inherent advantages, are liable to try to carry out cyber-attacks; and

5) **anarchists** opposed to the existing establishment who are interested in undermining it from within and without, and who endeavor to attack the entire system of computerization, which today is the basis for managing life as we know it, in order to disrupt or even destroy states' current social order and their fabric of life.

Cyber offense has the potential to change society's balance of power

because it empowers those engaged in asymmetrical conflicts that operate from a position of inferiority, especially terrorist organizations. Capabilities in this sphere may enable them to attack installations, systemic processes, and sites while causing heavy physical damage and wielding a significant psychological impact on the society and public under attack. They thus acquire capabilities other than those familiar from conventional terrorist attacks, such as suicide bombings, booby traps, hostage situations, hijackings, and kidnappings.

Cyber offense affords several advantages

First, it removes the necessity of physical presence at the target. It is possible to damage communications networks and control systems of installations and processes from afar and thus avoid physical barriers and human systems.

Second, it affords a wider scope of damage. Cyber-attacks occur not only in the physical space but also carry the potential for severe and sustained damage to control and infrastructure systems. Thus, while most conventional terrorist attacks are limited in time and space, a cyber attack magnifies terrorism's psychological impact through fear and intimidation.

Third, it is easier to conceal the identity and source of the attack; in cyberspace, identities and boundaries between states are more easily blurred. Terrorists attacking in cyberspace can not only conceal their identity but can also feed false information as to the source of the attack, for example, by attacking a site inside the target state using addresses of a friendly nation.

Fourth, cyberspace attacks are cost effective. Using the cyber platform for attacks maximizes the cost-benefit ratio from the perspective of a terrorist organization, endowed with fewer resources and capabilities than the states it targets. Assuming that terrorist organizations would prefer less defended targets rather than well-protected ones, they presumably would be able to gain access and insert malicious code into target sites, or use technologies that are becoming ever more accessible to wider audiences.

Fifth, cyber terrorism can be non-lethal. It can cause significant damage without direct fatalities or physical injury, granting terrorists success by means of intimidation and disruption of the routine. This gives the perpetrators the ability to devise a defense and logical explanations for their deeds, which after all did not spill blood but were only an indirect cause of lost lives. The innovativeness represented by such action would also garner terrorist organizations widespread media coverage and enable them to engage in non-lethal threats in which a price would be extorted in exchange for removing the threat of a cyber-attack.

It has been claimed that terrorist organizations are not interested in cyberspace because they prefer showcase attacks with much higher visibility rather than the anonymity that supposedly is conferred by attacks in this domain.

However this claim does not take into account the basic rationale of terrorism strategy, which holds that terrorist activity should focus on minimizing the power differential in the struggle against a stronger enemy with more powerful means, carry out destructive actions while identifying the weaknesses in the enemy's defense, and achieve a position of superiority at tolerable costs given the relatively poor means at the disposal of the perpetrators. Already today global jihad terrorist organizations are making use of cyberspace, though still in limited and relatively undeveloped fashion, to realize these advantages.

A study examining the cyberspace warfare capabilities of jihadist organizations identified a number of major features that serve to build and improve the organizational and operational infrastructures of terrorist organizations in the following fields:

Propaganda: using the web to disseminate ideas, decrees, directives, speeches, and opinion pieces by clergy and terrorist leaders.

Recruitment and training: using the web to identify and recruit potential members as well as to transmit instructional and training materials.

Fundraising and financing: using the web to fundraise under the guise of charities and aid organizations as well as to steal identities and credit cards.

Communications: using the web for operational communications while employing a range of tools, including accessible encryption tools.

Identifying targets and intelligence: using information available on the

web to identify targets and gather intelligence.

It is thus clear that an essential upgrade of cyberspace tools available to terrorist organizations, from logistical and propaganda tools to actual operational tools, is liable to generate an innovative, dramatic, and relatively cheap type of attack with the power to effect severe damage, even if carried out with a low signature or in total anonymity. Therefore every terrorist organization, especially one seeking fame and wanting to affect the public psyche and morale in the targeted enemy, sees such an attack as an important and worthy challenge. Innovation would also guarantee the perpetrators international fame and transform them into role models.

Thus, sub-state entities with more limited technological capabilities than the nations with which they are at war are liable to join the trend of using advanced technology needed for cyber warfare for their own benefit, either by receiving assistance from supportive nations or by acquiring such capabilities themselves in the future, by recruiting and operating individuals with the necessary skills in this field.

As for states supporting terrorism, cyberspace is very attractive for use of proxy organizations because of the anonymity afforded by the domain, the difficulty in proving the identity of the perpetrator, the high level of deniability by states about their involvement, and the satisfaction of causing severe damage to the enemy. Even if suspicions are aroused, it is still hard to prove guilt. Furthermore, the public under attack may perceive a cyber-attack to be less outrageous than a terrorist attack that employs firearms and causes direct death and destruction - even if the damage caused is greater, more destructive of property, and takes more lives than a violent terrorist act.

Despite these advantages of cyber-attacks, to date no such attack has been traced to a terrorist organization. Development of significant capabilities in this field requires surmounting a considerable intelligence and technological threshold. At this stage one may assume that terrorist organizations find it hard to identify, harness, and maintain such high technological capabilities and access that would allow them to cross that bar.

It is true that this limitation can be partially overcome through the assistance of state supporters of terrorism, but at least for now this is not enough to give terrorist organizations the significant, stable technological platform required for maintaining effective cyber-attack capabilities. In addition, terrorist organizations face limitations posed by cyber surveillance and state intelligence and technological capabilities that enable them to identify suspicious conduct on the web, identify attempts at organization, and mount a defense against them and against threats to specific targets.

Weaknesses and Responses

Although to date terrorist organizations have not been able to overcome the difficulties in achieving offensive cyber capabilities, civilian systems and routine civilian life presumably remain their preferred targets, because these are much more difficult to protect than security systems. Strengthening defenses of critical national infrastructures such as electric, water, and communications supply networks would likely encourage terrorists to seek out less protected targets in the civilian and commercial sectors. Even though systems in these sectors are usually not included in the rubric of critical and protected infrastructures, from the terrorist perspective an attack against them could be effective, by breaching ordinary citizens' basic sense of security and enhancing the terrorists' image by instilling fear.

A significant part of constructing a defense against cyber-attacks is general and independent of the source of the threat, whether terrorist, state or criminal. This is reflected organizationally - consider Israel's Information Security Authority and ministries specializing in cyber defense in various nations - and also in certain components of defense from the fields of information systems and general security. In contrast, in fighting terrorist organizations it is also necessary to activate two designated components that require sustained development and improvement.

The first is intelligence. Effective gathering of accurate, high quality intelligence requires using a range of sources including open sources and material from the terrorists' own computers and networks.

To this end it is necessary to develop capabilities of infiltrating these systems covertly and inserting information effectively and continuously. The challenge that must be overcome is the widespread global deployment typical of terrorist organizations that use many chat rooms and transmit messages using

unique code words. Intelligence agencies must be able to intercept these transmissions and decode them within the relevant timeframes and at the same time provide cyber defense systems with the tools needed to protect against and even disrupt the planned actions.

The second component is disruption. Unlike defense systems, which do not try to prevent an attack but rather obstruct its success once it has already been launched, the goal of disruption is to thwart the execution of the attack or to hamper its progress. Establishing an effective disruption structure against cyber-attacks by terrorist organizations requires intelligence monitoring and control that can identify the organization of an attack before it takes place and operate effectively to foil it. This aspect relies primarily on tactical intelligence gathering capabilities, both from computers and from communications networks used by terrorist organizations.

Disruption attempts can also be directed towards damaging the organizational infrastructures of the organization. An example of this occurred in England when British intelligence hacked the online issue of the British al-Qaeda magazine Inspire. In addition, in recent years the various components of the electronic jihad have been targeted for occasional cyber-attacks largely attributed to Western governments: the Taliban's website has been hacked time and again, as have exclusive jihadist forums and high profile fundamentalist websites. Meanwhile, American, Saudi Arabian, and Dutch authorities have extracted valuable information about potential Islamic terrorism from jihadist websites serving as honey traps for high quality intelligence.

At the same time, it is necessary to deepen the defenses of civilian systems that represent the greatest weakness and therefore are also preferred terrorist targets. For example, the British government began taking legislative steps that include authorizing the use of invasive techniques such as telephone wiretaps, surveillance of emails in police files connected to crimes of terrorism, torpedoing internet radicalization processes, and specialized training of police units to confront cyber threats. Nonetheless, in most states the defense of civilian systems is still in its infancy.

Most states' cyber defense resources are allocated to security systems and to what are considered critical national infrastructures. Deepening the defense of civilian systems requires radical changes on a national scale that must be supported by appropriate regulation.

Conclusion

"In December 2001, at a meeting in New York shortly after the 9/11 attacks, the philosopher Jacques Derrida presented his understanding of the changes generated in the world as a result of those events. According to Derrida, the attacks were still part of the "archaic theater of violence," the real, visible world, in which events are still conducted in "clear and great order." However, according to him, cyberspace presents us with a more potent threat to our political and physical world; the dangers inherent in it change the relationship between terrorism, in the psychological and historical sense of a violent attack, and the concept of territory.

Now, in the new techno- scientific world, the threat we knew in the past as real has become an invisible, quiet, and swift threat, devoid of bloodshed, which, according to Derrida, is worse than the 9/11 attacks, which at least were directed against a known location at a particular point in time. Now we are facing a challenge that threatens the social and economic fabric of life that connects all of us and upon which all of us depend in every place and at every moment.

The rapid technological developments and innovations of recent years in the domain of cyberspace have indeed created a battlefield that simultaneously brings together many varied populations, local and international, representing a desirable target and fertile ground of activity by sub-state entities.

Since thus far there has been no known cyber-attack perpetrated by a terrorist organization, the threat does not seem acute. The challenge facing those who would try to use cyberspace for malicious purposes is three-pronged: attaining high level intelligence, the ability to crack computerized systems protected with advanced technology (or accessibility to such ability), and very high levels of calculation and computerization skills.

However, the advantages afforded by attaining cyberspace capabilities as described in this essay are liable to serve as an incentive for terrorists to develop, acquire, or harness such capabilities in the future. Gaining control of the

advanced technological and intelligence capabilities required in cyberspace is likely to give these elements who seek to seriously damage their enemies by causing massive destruction and sowing terror and intimidation in the public at large the ability to disrupt the normal routine of civilian life, undermine civilian trust in their governments, and of course gain valuable prestige and media stature.

Therefore, Western nations must work diligently to meet this threat and improve the effective intelligence and defensive capabilities of civilian systems; while at the same time construct accurate intelligence gathering capabilities and the ability to disrupt cyberspace organization and attack by terrorists. Neglecting the civilian cyberspace domain, which is an attractive target for terrorists, is liable to prove disastrous in the future and place security personnel, when the time comes, in the same position as that fictional Hollywood hero of Die Hard 2 trying to save airplanes from crashing using nothing other than improvised beacons."

Yoram Schweitzer *is head of the Terrorism and Low Intensity Conflict Program at INSS*

Dr. Col. (ret.) Gabi Siboni *is head of the Military and Strategic Affairs Program at INSS and head of the Cyber Warfare Program at INSS, which is supported by the Philadelphia-based Joseph and Jeanette Neubauer Foundation.*

Einav Yogev *is a research assistant at the Terrorism and Low Intensity Conflict Program at INSS.*

This article was first published in Military & Strategic Affairs journal. Volume 3, issue 3.

NATO Group To Publish Rules For Cyber Warfare

Source: http://www.huffingtonpost.com/2013/03/19/cyber-warfare-rulebook_n_2907801.html

Even cyberwar has rules, and one group of experts is putting out a manual to prove it.

Their handbook, due to be published later this week, applies the practice of international law to the world of electronic warfare in an effort to show how hospitals, civilians and neutral nations can be protected in an information-age fight.

"Everyone was seeing the Internet as the `Wild, Wild West,'" U.S. Naval War College Professor Michael Schmitt, the manual's editor, said in an interview before its official release. "What they had forgotten is that international law applies to cyberweapons like it applies to any other weapons."

The Tallinn Manual – named for the Estonian capital where it was compiled – was created at the behest of the NATO Cooperative Cyber Defense Center of Excellence, a NATO think tank. It takes existing rules on battlefield behavior, such as the 1868 St. Petersburg Declaration and the 1949 Geneva Convention, to the Internet, occasionally in unexpected ways.

Marco Roscini, who teaches international law at London's University of Westminster, described the manual as a first-of-its-kind attempt to show that the laws of war – some of which date back to the 19th century – were flexible enough to accommodate the new realities of online conflict.

The 282-page handbook has no official standing, but Roscini predicted that it would be an important reference as military lawyers across the world increasingly grapple with what to do about electronic attacks.

"I'm sure it will be quite influential," he said.

The manual's central premise is that war doesn't stop being war just because it happens online. Hacking a dam's controls to release its reservoir into a river valley can have the same

effect as breaching it with explosives, its authors argue.

Legally speaking, a cyberattack that sparks a fire at a military base is indistinguishable from an attack that uses an incendiary shell.

The humanitarian protections don't disappear online either. Medical computers get the same protection that brick-and-mortar hospitals do. The personal data related to prisoners of war has to be kept safe in the same way that the prisoners themselves are – for example by having the information stored separately from military servers that might be subject to attack.

Cyberwar can lead to cyberwar crimes, the manual warned. Launching an attack from a neutral nation's computer network is forbidden in much the same way that hostile armies aren't allowed to march through a neutral country's territory. Shutting down the Internet in an occupied area in retaliation for a rebel cyberattack could fall afoul of international prohibitions on collective punishment.

The experts behind the manual – two dozen officers, academics, and researchers drawn mainly from NATO states – didn't always agree on how traditional rules applied in a cyberwar.

Self-defense was a thorny issue. International law generally allows nations to strike first if they spot enemy soldiers about to pour across the border, but how could that be applied to a world in which attacks can happen at the click of a mouse?

Other aspects of international law seemed obsolete – or at least in need of an upgrade – in the electronic context.

Soldiers are generally supposed to wear uniforms and carry their arms openly, for example, but what relevance could such a requirement have when they are hacking into distant targets from air-conditioned office buildings?

The law also forbids attacks on "civilian objects," but the authors were divided as to whether the word "object" could be interpreted to mean "data." So that may leave a legal loophole for a military attack that erases valuable civilian data, such as a nation's voter registration records.

Hackers attack European governments using 'MiniDuke' malware

Source: http://www.guardian.co.uk/technology/2013/feb/27/hackers-attack-european-governments-miniduke

Cyber criminals have targeted government officials in more than 20 countries, including Ireland and Romania, in a complex online assault seen rarely since the turn of the millennium.

The attack, dubbed "MiniDuke" by researchers, has infected government computers as recently as this week in an attempt to steal geopolitical intelligence, according to security experts.

MiniDuke is the latest in a string of cyber attacks aimed at governments and other high-profile institutions, following revelations about the suspected Chinese hacking of western defence and media organisations.

Unusually, security researchers said there was no clear indication of who was behind the latest online attack.

The cybersecurity firm Kaspersky Lab, which discovered MiniDuke, said the attackers had servers based in Panama and Turkey – but an examination of the code revealed no further clues about its origin.

Goverments targeted include those of Ireland, Romania, Portugal, Belgium and the Czech Republic. The malware also compromised the computers of a prominent research foundation in Hungary, two thinktanks, and an unnamed healthcare provider in the US.

Victims' computers were infected when they opened a cleverly disguised Adobe PDF attachment to an email. The document would be tailored specifically to its target, according to the researchers, as unsuspecting government victims are more likely to open an attachment that mentioned foreign policy, a human rights seminar, or Nato membership plans.

Once it was opened, the MiniDuke malware would install itself on a victim's computer. It is not known what information the attackers are targeting. "It's currently unclear what the attackers were after. But the interest in these high-profile victims is quite obvious," said Vitali Kamluk, chief malware expert at Kaspersky Lab.

Eugene Kaspersky, founder and chief executive of Kaspersky Lab, said MiniDuke had the potential to be "extremely dangerous" because it was an "elite, old-school" attack that used some 21st century tricks.

"This is a very unusual cyber attack," he said. "I remember this style of malicious programming from the end of the 1990s and the beginning of the 2000s. I wonder if these types of malware writers, who have been in hibernation for more than a decade, have suddenly awoken and joined the sophisticated group of threat actors active in the cyber world."

Expert says 10,000 extremist websites on the web

Source:http://www.terrorismwatch.org/2013/03/expert-says-10000-extremist-websites-on.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+terrorismwatch%2FJTvK+%28Terrorism+Watch%29&utm_content=Yahoo!+Mail

There are more than 10,000 extremist websites on the Internet compared to fewer than 100 countering them, an analyst Tuesday told a conference which stressed the need to rebut militant propaganda.

"In many ways, the terrorists are very successful in cyberspace," said counter-terrorism analyst Rohan Gunaratna, who heads the International Centre for Political Violence and Terrorism Research in Singapore. "It is very important for us to build in the next 10 years the capacities and capabilities to counter the increasing presence and the operation of these groups in cyberspace."

Speakers at the International Conference on Terrorist Rehabilitation and Community Resilience said moderate Islamic groups and governments should make a concerted effort to counter extremist propaganda on the Internet.

YouTube, Facebook, Twitter and other social media are increasingly being exploited to spread extremist views, and moderate religious leaders and governments must keep pace to counter their arguments, they said.

Singapore Prime Minister Lee Hsien Loong said in a keynote speech that self-radicalisation through constant exposure to radical views online was a "growing phenomenon".

"Jihadist sites and sermons by charismatic ideologue firebrands are just a mouse click away," said Lee, who also stressed the need for closer international cooperation against terrorism.

Some 500 security analysts, academics and religious leaders attended the forum.

Islamic scholar Ali Mohamed, co-chairman of Singapore's Religious Rehabilitation Group (RRG), said cyberspace "is shaping up to be the new battleground for hearts and minds".

The RRG counsels and reindoctrinates jailed militants and helps them reintegrate into society, including some arrested in late 2001 for allegedly plotting to bomb US and other targets in the city-state.

"Terrorists are increasingly exploiting the Internet as a tool for mass communication and radicalisation," said Ali.

"RRG believes that this is one of our greatest challenges today -- to deal (with) and counter the pervasive spread of terrorist ideologies and extremist views online."

What if they pulled the plug?

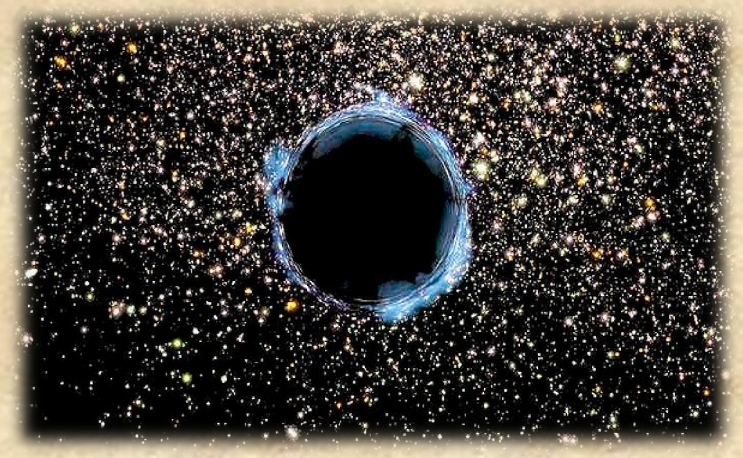
Source:http://www.smh.com.au/it-pro/security-it/what-if-they-pulled-the-plug-20130327-2gun9.html?utm_source=+Synergic+Cyber+Attacks&utm_campaign=ACD%2FEWI+BLOG&utm_medium=email

Two major recent attacks on the Internet give us just a hint of what to expect if/when our economic and financial infrastructures are hit by different attacks at once.

Cyberbunker - not a Chinese - but a Dutch webhosting company generated the largest global distributed denial of service (DDoS) attack on the spam filtering company, Spamhouse.

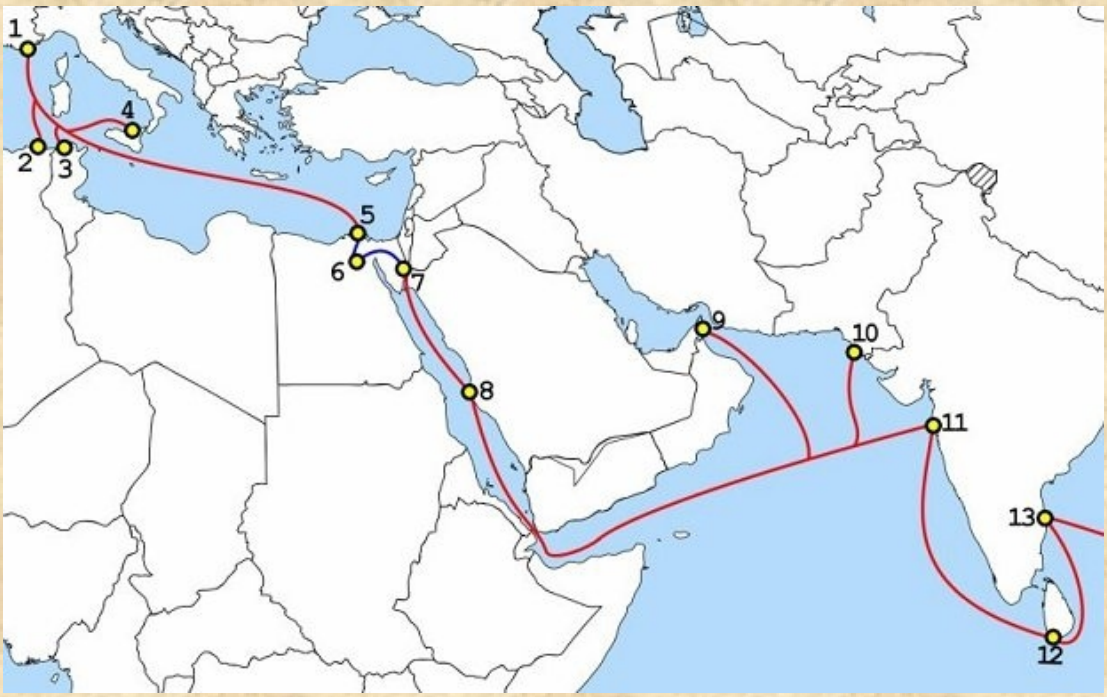
What is said to be a dispute between Cyberbunker and Spamhouse caused the global disruption of Internet

services, which according to the Moscow based Kaspersky Lab, is going to get worse. "Such DDoS attacks may affect regular users



as well, with network slowdown or total unavailability of certain Web resources...There may be further disruptions on a larger scale as the attack escalates."

A different kind of attack was committed by three men just 820 yards offshore Alexandria, Egypt. They were caught



cutting the 12,500 miles long South East Asia-Middle East-West Europe 4 (SEA-ME-WE 4) cable (photo) that goes from France to Singapore. Internet services were disturbed in Italy, Algeria, Tunisia, Egypt, United Arab Emirates, Saudi Arabia, Sudan, Uganda, Kenya, Tanzania, Malaysia, Thailand, Bangladesh, India, Sri Lanka and Pakistan.

Judging by the ease by which both attacks have been carried out, it is clear that physical and cyber security are wanting, and that preparedness for a combined attack is lacking. It seems that such an emerging threat is too complex or not yet fully understood, thus leaving us unprepared.

A major obstacle that hinders the development of proper security measures, especially on the cyber front, is the timidity of affected companies to admit they have been attacked. There is also a tendency to minimize the threat; short temporary disruptions are attributed to glitches in the system until a massive attack is undeniable. Such obstructions render ineffective the supposed close monitoring of misuse, or unlawful conduct in financial and economic sectors.

The weapons of this new war are not as easily identifiable as Korean ballistic missiles, or Iranian nuclear powers.

They can be used instantaneously or incrementally over time and be hardly noticed. Even when sporadic attacks are noticed, analytical methods may fail to recognize the potential of a large-scale attack, or the perpetrators. However, difficulties in establishing identification and lack of cooperation prevents

decision makers from developing better detection and prevention systems, or advanced methods to respond to them.
This new economic warfare presents a nascent threat in complex areas that challenge analysis and identification. While at first our streets will not be littered with bodies as with a nuclear attack, a stealth attack on our economic, financial and communication channels, could in short time destroy the U.S. economy and devastate its people. Perhaps it's time to rethink our mostly Digital depended economy.

How Spamhaus' attackers turned DNS into a weapon of mass destruction

By Sean Gallagher

Source: http://arstechnica.com/information-technology/2013/03/how-spamhaus-attackers-turned-dns-into-a-weapon-of-mass-destruction/

Aurich Lawson

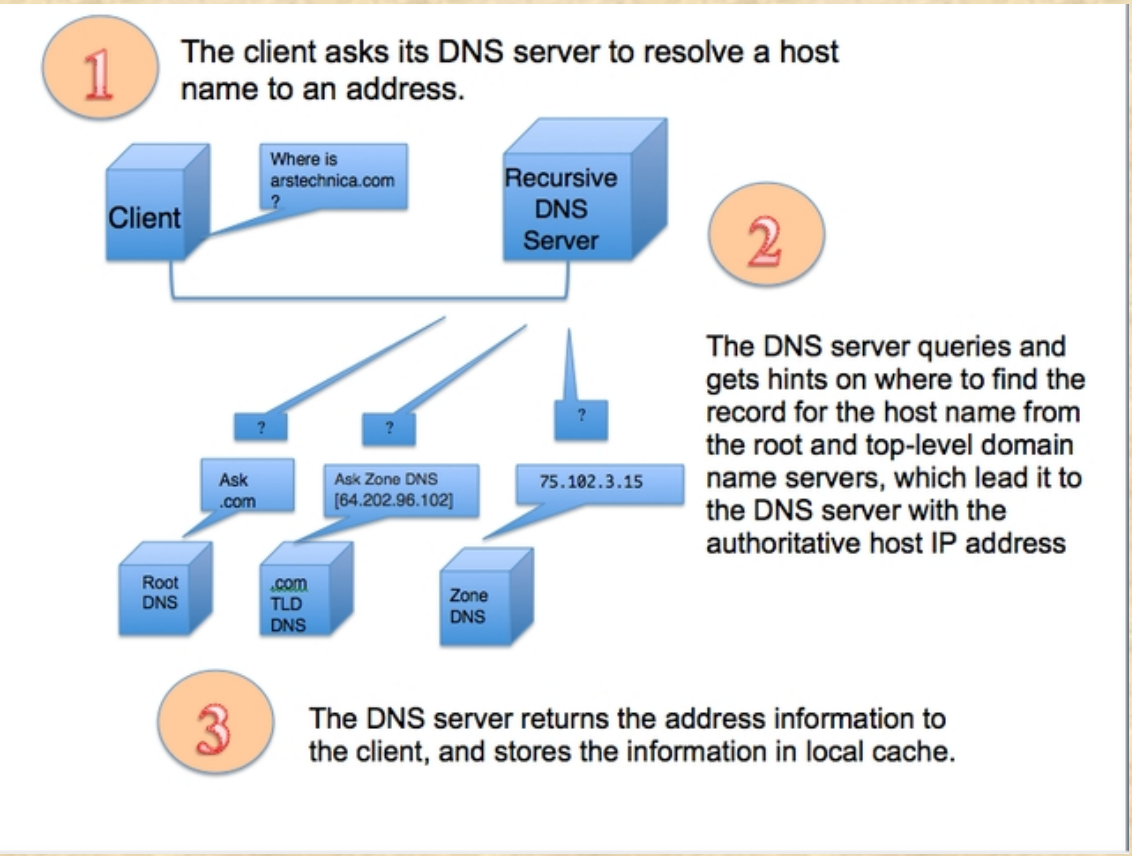
A little more than a year ago, details emerged about an effort by some members of the hacktivist group Anonymous to build a new weapon to replace their aging denial-of-service arsenal. The new weapon would use the Internet's Domain Name Service as a force-multiplier to bring the servers of those who offended the group to their metaphorical knees. Around the same time, an alleged plan for an Anonymous operation, "Operation Global Blackout" (later dismissed by some security experts and Anonymous members as a "massive troll"), sought to use the DNS service against the very core of the Internet itself in protest against the Stop Online Piracy Act.
This week, an attack using the technique proposed for use in that attack tool and operation—both of which failed to materialize—was at the heart of an ongoing denial-of-service assault on Spamhaus, the anti-spam clearing house organization. And while it hasn't brought the Internet itself down, it has caused major slowdowns in the Internet's core networks.
DNS Amplification (or DNS Reflection) remains possible after years of security expert warnings. Its power is a testament to how hard it is to get organizations to make simple changes that would prevent even recognized threats. Some network providers have made tweaks that prevent botnets or "volunteer" systems within their networks to stage such attacks. But thanks to public cloud services, "bulletproof" hosting services, and other services that allow attackers to spawn and then reap hundreds of attacking systems, DNS amplification attacks can still be launched at the whim of a deep-pocketed attacker—like, for example, the cyber-criminals running the spam networks that Spamhaus tries to shut down.

Hello, operator?

The Domain Name Service is the Internet's directory assistance line. It allows computers to get the numerical Internet Protocol (IP) address for a remote server or other network-attached device based on its human-readable host and domain name. DNS is organized in a hierarchy; each top-level domain name (such as .com, .edu, .gov, .net, and so on) has a "root" DNS server keeping a list of each of the "authoritative" DNS servers for each domain registered with them. If you've ever bought a domain through a domain registrar, you've created (either directly or indirectly) an authoritative DNS address for that domain by selecting the primary and secondary DNS servers that go with it.

When you type "arstechnica.com" into your browser's address bar and hit the return key, your browser checks with a DNS resolver—your personal Internet 411 service— to determine where to send the Web request. For some requests, the resolver may be on your PC. (For example, this happens if you've requested a host name that's in a local "hosts" table for servers within your network, or one that's stored in your computer's local cache of DNS addresses you've already looked up.) But if it's the first time you've tried to connect to a computer by its host and domain name, the resolver for the request is probably running on the DNS server configured for your network—within your corporate network, at an Internet provider, or through a public DNS service such as Google's Public DNS.

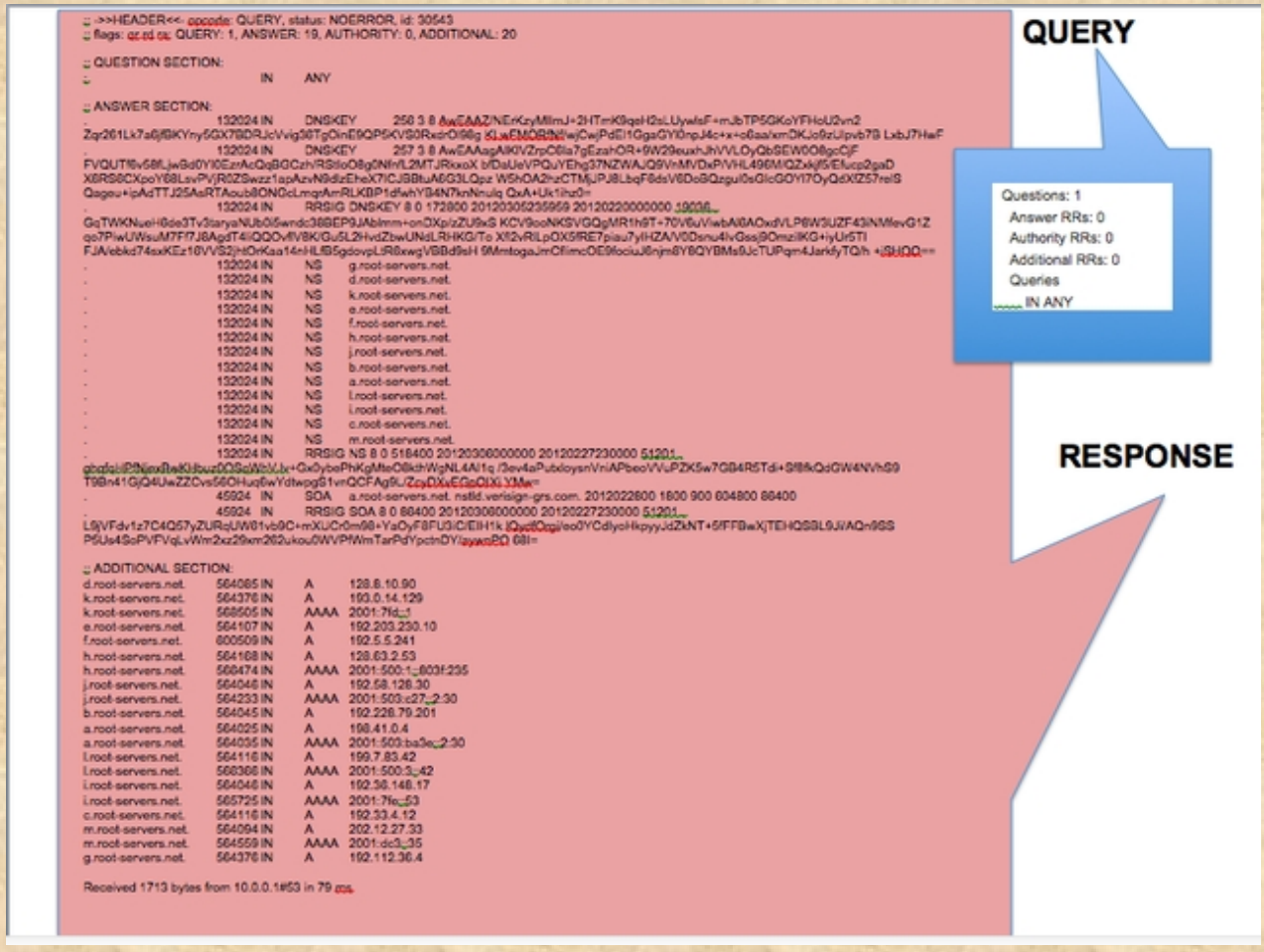
There are two ways for a resolver to get the authoritative IP address for a domain name that isn't in its cache: an iterative request and a recursive request. In an iterative request, the resolver pings the top-level domain's DNS servers for the authoritative DNS for the destination domain, then it sends a DNS request for the full hostname to that authoritative server. If the computer that the request is seeking is in a subdomain or "zone" within a larger domain—such as www.subdomain.domain.com—it may tell the resolver to go ask that zone's DNS server. The resolver "iterates" the request down through the hierarchy of DNS servers until it gets an answer.



But on some networks, the DNS resolver closest to the requesting application doesn't handle all that work. Instead, it sends a "recursive" request to the next DNS server up and lets that server handle all of the walking through the DNS hierarchy for it. Once all the data is collected from the root, domain, and

subdomain DNS servers for the requested address, the resolver then pumps the answer back to its client.

How DNS queries are supposed to work—when they're not being used as weapons.



To save time, DNS requests don't use the "three-way handshake" of the Transmission Control Protocol (TCP) to make all these queries. Instead, DNS typically uses the User Datagram Protocol (UDP)—a "connectionless" protocol that lets the server fire and forget requests.

Pump up the volume

That makes the sending of requests and responses quicker—but it also opens up a door to abuse of DNS that DNS amplification uses to wreak havoc on a target. All the attacker has to do is find a DNS server open to requests from any client and send it requests forged as being from the target of the attack. And there are millions of them.

The "amplification" in DNS amplification attacks comes from the size of those responses. While a DNS lookup request itself is fairly small, the resulting response of a recursive DNS lookup can be much larger. A relatively small number of attacking systems sending a trickle of forged UDP packets to open DNS servers can result in a firehose of data being blasted at the attackers' victim.

DNS amplification attacks wouldn't be nearly as amplified if it weren't for the "open" DNS servers they use to fuel the attacks. These servers have been configured (or misconfigured) to answer queries from addresses outside of their network. The volume of traffic that can be generated by such open DNS servers is huge. Last year, Ars reported on a paper presented by Randal Vaughan of Baylor University and Israeli security consultant Gadi Evron at the 2006 DefCon security conference. The authors documented a series of DNS amplification attacks in late 2005 and early 2006 that generated massive traffic loads for the routers of their victims. In one case, the traffic was "as high as 10Gbps and used as many as 140,000 exploited name servers," Vaughan and Evron reported. "A DNS query consisting of a 60 byte request can be answered with responses of over 4000 bytes, amplifying the

response packet by a factor of 60."

But even if you can't find an open DNS server to blast recursive responses from, you can still depend on the heart of the Internet for a respectable hail of packet projectiles. A "root hint" request—sending a request for name servers for the "." domain—results in a response 20 times larger than the packet the request came in. That's in part thanks to DNS-SEC, the standard adopted to make it harder to spoof DNS responses, since now the response includes certificate data from the responding server.

A comparison of a "root hint" query and the response delivered by the DNS server. Not all data shown.

Sean Gallagher

In the case of the attack on Spamhaus, the organization was able to turn to the content delivery network CloudFlare for help. CloudFlare hid Spamhaus behind its CDN, which uses the Anycast feature of the Border Gateway Protocol to cause packets destined for the antispam provider's site to be routed to the closest CloudFlare point of presence. This spread out the volume of the attack. And CloudFlare was able to then shut off amplified attacks aimed at Spamhaus with routing filters that blocked aggregated DNS responses matching the pattern of the attack.

But that traffic still had to get to Cloudflare before it could be blocked. And that resulted in a traffic jam in the core of the Internet, slowing connections for the Internet as a whole.

No fix on the horizon

The simplest way to prevent DNS amplification and reflection attacks would be to prevent forged DNS requests from being sent along in the first place. But that "simple" fix isn't exactly easy—or at least easy to get everyone who needs to participate to do.

There's been a proposal on the books to fix the problem for nearly 13 years—the Internet Engineering Task Force's BCP 38, an approach to "ingress filtering" of packets. First pitched in ~~2000~~ 1998 as part of RFC 2267 , the proposal has gone nowhere. And while the problem would be greatly reduced if zone and domain DNS servers simply were configured not to return recursive or even "root hint" responses received from outside their own networks, that would require action by the owners of the network. It's an action that doesn't have a direct monetary or security benefit to them associated with it.

ISPs generally do "egress filtering"—they check outbound traffic to make sure it's coming from IP addresses within their network. This prevents them from filling up their peering connections with bad traffic. But "ingress" filtering would check to make sure that requests coming in through a router were coming from the proper direction based on their advertised IP source.

Another possible solution that would eliminate the problem entirely is to make DNS use TCP for everything—reducing the risk of forged packets. DNS already uses TCP for tasks like zone transfers. But that would require a change to DNS itself, so it's unlikely that would ever happen, considering that you can't even convince people to properly configure their DNS servers to begin with.

Maybe the attack on Spamhaus will change that, and core network providers will move to do more to filter DNS traffic that doesn't seem to match up with known DNS servers. Maybe just maybe, BCP 38 will get some traction. And maybe pigs will fly.

Sean Gallagher *is the IT editor at Ars Technica. A University of Wisconsin grad, he wrote his first program in high school on a DEC PDP-10, and his first database app on a dual-floppy Apple II. Sean's first paid writing gig was producing "supplemental content" for Microprose's Gunship 2000 and F-117 Stealth Fighter 2.0 game manuals. A former naval officer, Sean served aboard the USS Iowa (BB-61) and at a river patrol boat squadron— where discovery of his computer skills landed him the assignments of network administrator and computer security officer. Aside from a few dark years as a systems integrator and a stint as Ziff Davis Enterprise's director of IT strategy, Sean has been either in the review lab or on a tech beat for most of the last two decades. A telecommuter since 1995, Sean lives and works in Baltimore.*

Cyber-attackers out to destroy data and not just disable it

By David E. Sanger and Nicole Perlroth (The New York Times)
Source:http://www.terrorismwatch.org/2013/03/cyber-attackers-out-to-destroy-data-and.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+terrorismwatch%2FJTvK+%28Terrorism+Watch%29&utm_content=Yahoo!+Mail

American Express customers trying to gain access to their online accounts Thursday were met with blank screens or an ominous ancient type face. The company confirmed that its website had come under attack.

The assault, which took American Express offline for two hours, was the latest in an intensifying campaign of unusually powerful attacks on U.S. financial institutions that began last September and have taken dozens of them offline intermittently, costing millions of dollars.

JPMorgan Chase was taken offline by a similar attack this month. And last week, a separate, aggressive attack incapacitated 32,000 computers at South Korea's banks and television networks.

The culprits of these attacks, officials and experts say, appear intent on disabling financial transactions and operations.

Corporate leaders have long feared online attacks aimed at financial fraud or economic espionage, but now a new threat has taken hold attackers, possibly with state backing, who seem bent on destruction.

"The attacks have changed from espionage to destruction," said Alan Paller, director of research at SANS, a cybersecurity training organization. "Nations are actively testing how far they can go before we will respond."

Security experts who studied the attacks said they were part of the same campaign that took down the websites of Wells Fargo, Bank of America and others over the past six months. A group that calls itself the Izz ad-Din al-Qassam Cyber Fighters has claimed responsibility for those attacks.

The group says it is retaliating for an anti-Islamic video posted on YouTube last fall. But U.S. intelligence officials and industry investigators say they believe that the group is a convenient cover for Iran. Just how tight the connection is - or whether the group is acting on direct orders from the Iranian government - is unclear. Government officials and bank executives have failed to produce a smoking gun.

North Korea is considered the most likely source of the South Korean attacks, although investigators are still struggling to follow the digital trail, a process that could take months. The North Korean government of Kim Jong Un has openly declared that it is seeking out online targets in its neighbor to the south to exact economic damage.

Representatives of American Express confirmed that the company was under attack Thursday but said that there was no evidence that customer data had been compromised. An FBI spokesman did not respond Thursday to a request for comment about the American Express attack.

Spokesmen for JPMorgan Chase said they would not talk about the recent attack there, its origins or its consequences.

The largest contingent of instigators of attacks in the private sector, government officials and researchers say, remains Chinese hackers intent on stealing corporate secrets. But the U.S. and South Korean bank attacks underscore a growing fear that the two countries now worrying banks, oil producers and governments may be Iran and North Korea, not because of their skill but because of their brazenness.

Neither country is considered a superstar in this area. But the appeal of digital weapons is similar to that of nuclear capability: It is a way for an outgunned, outfinanced nation to even the playing field.

"These countries are pursuing cyberweapons the same way they are pursuing nuclear weapons," said James A. Lewis, a computer security expert at the Center for Strategic and International Studies in Washington. "It's primitive; it's not top of the line, but it's good enough, and they are committed to getting it."

U.S. officials are weighing their response options, but the issues involved are complex.

At a meeting of banking executives, regulators and representatives from the Homeland Security and Treasury departments in December, some attendees pushed the United States to hit back at the hackers, while others argued that doing so would only lead to more aggressive attacks, according to two people at the meeting.

The difficulty of deterring such attacks was also the focus of a White House meeting earlier this month with President Barack Obama and business leaders including Jamie Dimon, chief executive of JPMorgan Chase; Brian T. Moynihan of Bank of America; Rex W. Tillerson of Exxon Mobil; Randall L. Stephenson of AT&T and others.

Obama's goal was to erode the business community's intense opposition to federal legislation that would give the government oversight of how companies protect "critical infrastructure," like banking systems and energy and cellphone networks. That opposition killed a bill last year, prompting Obama to sign an executive order promoting increased information-sharing with businesses.

"But I think we heard a new tone at this latest meeting," an Obama aide said later. "Six months of unrelenting attacks have changed some views."

Lewis, the cybersecurity expert, agreed.

"The Iranian attacks have tilted private sector opinion," he said. "Hence the muted reaction to the executive order versus squeals of outrage. Companies are much more concerned about this and much more willing to see a government role."

When hackers believed by U.S. intelligence officials to be Iranians hit the world's largest oil producer, Saudi Aramco, last year, they did not just erase data on 30,000 Aramco computers; they replaced the data with an image of a burning U.S. flag. In the assault on South Korea last week, some affected computers displayed an ominous image of skulls.

"This attack is as much a cyber-rampage as it is a cyberattack," Rob Rachwald, a research director at FireEye, a computer security firm, said of the South Korea attacks.

In the past, such assaults typically occurred through a denial-of-service attack, in which hackers flood their target with Web traffic from networks of infected computers until it is overwhelmed and shuts down. One such case was a 2007 Russian attack on Estonia that affected Estonian banks, the Parliament, ministries, newspapers and broadcasters and nearly crippled the small Baltic nation.

With their campaign against U.S. banks, the hackers suspected of being Iranian have taken that kind of attack to the next level. Instead of using individual personal computers to send Web traffic to each bank, they infected powerful, commercial data centers with sophisticated malware and instructed them to simultaneously fire at each bank, giving them the horsepower to inflict a huge attack.

As a result, the hackers were able to take down the consumer banking sites of American Express, JP Morgan Chase, Bank of America, Wells Fargo and other banks with exponentially more traffic than hit Estonia in 2007.

In the attack on Saudi Aramco last year, the culprits did not mount that type of assault; instead, they created malware designed for greatest effect, coded to spread to as many computers as possible.

Likewise, the attacks last week on South Korean banks and broadcasters were far more sophisticated than coordinated denial-of-service attacks in 2009 that briefly took down the websites of South Korea's president and its Defense Ministry and those of the U.S. Treasury Department, the Secret Service and the Federal Trade Commission. Those attacks were mostly annoyances; they largely did not affect operations.

But this time around in South Korea, the attackers engineered malware that could evade popular South Korean anti-virus products, spread it to as many computer systems as possible, and inserted a time bomb to take out all the systems at once for greatest impact.

The biggest concern, Lewis said "We don't know how they make decisions. When you add erratic decision making, then you really have something to worry about."