North Korea is playing dangerous games !

CBRNE Newsletter Terrorism

Volume 47, 2013

Cyber News

www.cbrne-terrorism-newsletter.com

Cyber security in 2013: How vulnerable to attack is US now?

By Mark Clayton

Source: http://www.csmonitor.com/USA/2013/0109/Cyber-security-in-2013-How-vulnerable-to-attack-is-US-now-video

The phalanx of cyberthreats aimed squarely at Americans' livelihood became startlingly clear in 2012 – and appears poised to proliferate in 2013 and beyond as government officials, corporate leaders, security experts, and ordinary citizens scramble to devise protections from attackers in cyberspace.

Some Americans came screen to screen with such threats via their smart phones, discovering malicious software (malware) designed to steal their credit-card numbers, account passwords, and even the answers to their secret security questions. Others were temporarily blocked from accessing their bank accounts online, as US bank websites came under major attack at least twice in 2012 by a hacker group with possible ties to Iran. Some citizens learned that their home PCs had become infected by "ransomware," which locks up a computer's operating system until the bad guys get paid – and often even afterward.

But personal inconvenience is only the beginning. Homeland security is also at stake. The US government in 2012 learned that companies operating natural gas pipelines were under cyberattack, citing evidence that cyberspies, possibly linked to China, were infiltrating the companies' business networks. Those networks, in turn, are linked to industrial systems that control valves, switches, and factory processes. Utilities that operate the nation's electric grid are known to have been another target, as are US tech companies. Crucial government agencies, such as the Pentagon and the Federal Trade Commission, are also targets.

It all adds up to growing evidence – recognized to varying degrees by the US public, politicians, and businesses – that cybersecurity is the next frontier of national security, perhaps second only to safeguarding the nation against weapons of mass destruction.

"The cyberthreat facing the nation has finally been brought to public attention," says James Lewis, a cybersecurity expert with the Center for Strategic and International Studies (CSIS), a Washington national-security think tank. "Everyone knows it's a problem. It has moved out of the geek world, and that's a good thing. But it's led to more confusion than clarity. So now we're developing the skills to talk about it – and it's taking longer than I thought it would."

The awakening to cyberthreats has been gradual. In 2010, news of the world's first cyberweapon – the Stuxnet computer worm that attacked part of Iran's nuclear fuel program – burst upon the scene, raising concern about broad replication. Then came an increasing onslaught from hacktivist groups, which often stole and released private data. Between December 2010 and June 2011, for example, members of Anonymous were responsible for cyberattacks against the websites of Visa, MasterCard, and PayPal, as part of a tit for tat over the controversial WikiLeaks website.

Last year came the bald warning from Defense Secretary Leon Panetta of the possibility of a "cyber Pearl Harbor" – perhaps perpetrated by an enemy nation, extremist hacktivist groups, or cyber-savvy terrorists – that could be destructive enough to "paralyze the nation."

The threats originate from any number of sources: the lone hacker in the basement, networks of activists bent on cyber-monkey-wrenching for a cause, criminal gangs looking to steal proprietary data or money, and operatives working for nation-states whose intent is to steal, spy, or harm.

But at the Pentagon, attention these days is focused on the advancing cyberwar capabilities of China, Russia, and, especially, Iran. Iranian-backed cyberattackers, who in September targeted nine US banks with distributed denial-of-service attacks that temporarily shut down their websites, were testing America's reaction, Dr. Lewis says. The same kind of attack took place in December.

All the multiple attackers with various motives – and multiple targets – make defending against cyberattacks a challenge. Government agencies, the Pentagon, and defense contractors seem to have gotten serious and have greatly beefed up security. Companies' spending data

also indicate an apparently growing awareness of the threat, with cybersecurity expenditures increasing.

But that's hardly enough, cyber experts such as Lewis say. Critical infrastructure needs to have its cybersecurity tested to ensure it's adequate, he and others say.

"Like anything else in America, there's a large, noisy debate driven by business interests and hucksterism – people shouting about cyberattacks," Lewis says. "But the situation is clearly serious. Our vulnerabilities are great. I recall our first CSIS meeting on cybersecurity in 2001. At that time, we agreed that if nothing significant was done to change things in a decade, we'd be in real trouble. Well, here we are."

What more to do?

Warnings such as the "Pearl Harbor" one from Mr. Panetta in October have stirred debate over further measures the United States should take to protect itself.

Congress recently grappled with legislation that would have allowed the Department of Homeland Security (DHS) to do cybersecurity testing on computer networks of companies that operate natural gas pipelines and other vital assets – and would have granted those companies protection from financial liability in the event of a cyberattack on their facilities. But lawmakers did not approve it, mainly on grounds that the business community objected to the expected high cost of the new mandates and regulations, as well as the exposure of proprietary information to government. In response, President Obama is expected to issue an executive order soon, though it won't give the federal government as much authority to conduct cyberdefense testing as the legislation would have.

Not everyone agrees on what defensive actions to take. Some see Panetta's words as hyperbole aimed mostly at preserving the defense budget. Others warn of a US policy "overreaction" in which Internet freedoms are stifled by Big Brother-style digital filters.

"As ominous as the dark side of cyberspace may be, our collective reactions to it are just as ominous – and can easily become the darkest driving force of them all should we over-react," writes Ron Deibert, a University of Toronto cyber researcher, in a recent paper titled "The Growing Dark Side of Cyberspace (... and What To Do About It)."

Still others doubt that America's cyberadversaries are as capable as they are made out to be. In Foreign Policy magazine in an article headlined "Panetta's Wrong About a Cyber 'Pearl Harbor,' " John Arquilla argues that the Defense secretary has employed the "wrong metaphor."

"There is no 'Battleship Row' in cyberspace," writes the professor of defense analysis at the Naval Postgraduate School in Monterey, Calif. "Pearl Harbor was a true 'single point of failure.' Nothing like this exists in cyberspace."

Scope of the damage

There's little question, though, that cyberthreats are already doing harm to the US economy – and may do even more.

"At a corporate level, attacks of this kind have the potential to create liabilities and losses large enough to bankrupt most companies," according to the US Cyber Consequences Unit, a think tank advising government and industry. "At a national level, attacks of this kind, directed at critical infrastructure industries, have the potential to cause hundreds of billions of dollars' worth of damage and to cause thousands of deaths."

Evidence of the damage includes the following:

• Cyberespionage that's intended to scoop up industrial secrets alone costs US companies as much as $400 billion annually, some researchers estimate. Much of that comes over the long term, as stolen proprietary data give firms in other nations, such as China, a leg up by slashing research-and-development costs.

• The volume of malicious software targeting US computers and networks has more than tripled since 2009, according to a 2011 report by the director of national intelligence. Reports in 2012 corroborate that upward trend.

• Ransomware netted cybercriminals $5 million last year, by some estimates. Smart-phone and other mobile cybervulnerabilities nearly doubled from 2010 to 2011, according to the cybersecurity firm Symantec.

• The Pentagon continues to report more than 3 million cyberattacks of various kinds each year on its 15,000 computer networks.

Defense contractors such as Lockheed Martin are key targets, too. At a November news conference, Chandra McMahon, Lockheed vice president and chief information security officer, revealed that 20 percent of all threats aimed at the company's networks were

sophisticated, targeted attacks by a nation or a group trying to steal data or harm operations. "The number of campaigns has increased dramatically over the last several years," Ms. McMahon said.

Perhaps topping the list of concerns, though, is the accelerating pace of cyberattacks on the computerized industrial control systems that run the power grid, chemical plants, and other critical infrastructure.

"We know that [nation-state cyberspies] can break into even very security-conscious networks quite regularly if not quite easily," says Stewart Baker, a former DHS and National Security Agency (NSA) cyber expert now in legal practice at Steptoe & Johnson. "Once there, they can either steal information or cause damage."

In 2009, US companies that own critical equipment reported nine such incidents to the Industrial Control Systems Cyber Emergency Response Team, an arm of the DHS. In 2011, they reported 198.

"The threats to systems supporting critical infrastructures are evolving and growing," the Government Accountability Office concluded in a July report on the US power grid's exposure to cyberattacks.

The potential impact of such attacks, the report continues, "has been illustrated by a number of recently reported incidents and can include fraudulent activities, damage to electricity control systems, power outages, and failures in safety equipment."

Some experts say the rise in such incidents may be exaggerated. "What's happening is that our ability to identify attacks is improving, not necessarily that numbers or strength [of the attacks] is getting worse," says Robert Huber, a principal at Critical Intelligence, a cybersecurity firm in Idaho Falls, Idaho, that specializes in protecting critical infrastructure.

An awakening

A seminal speech on cyberthreats by Mr. Obama in May 2009 marked the onset of heightened public awareness of the problem. Cybersecurity would for the first time become an administration priority, he said, with a White House cyber czar and a "new comprehensive approach to securing America's digital infrastructure."

"Cyberspace is real, and so are the risks that come with it," Obama said. "It's the great irony of our Information Age – the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

In particular, cybersecurity experts inside major corporations are becoming increasingly concerned. Corporate chief information security officers reported a 50 percent jump in the "measure of perceived risk" since March 2011, according to a cybersecurity index cocreated by Daniel Geer, chief information security officer of In-Q-Tel, the venture capital arm of the Central Intelligence Agency. In November, the index continued its upward march, rising 1.8 percent over the previous month.

Awareness is building among the public, too. Two-thirds of respondents to a national survey by the University of Oklahoma in February 2012 rated the threat of cyberwar at 6.5 on a scale where zero is "no threat" and 10 is "extreme threat." But only 1 in 3 rated themselves as having above-average knowledge about the cyberwar threat.

"These response patterns suggest a public that is aware of the emerging issue of cyber war, does not feel well informed about it, but perceives it to pose a substantial threat," the researchers reported.

Wariness and circumspection about cyberthreats are good first steps, cyber experts say, because they are the precursor to action. They say laws that require owners of critical infrastructure to meet cybersecurity performance standards are the next logical step.

"It's clear we have enemies who'd love to [attack US critical infrastructure], especially if they could escape blame for doing so," says Mr. Baker, the former NSA cyber expert. "It may not happen soon. But we would be crazy to assume it will never happen."

__Mark Clayton__ has written about energy and the environment from the Monitor's Boston bureau since 2003 and cyber-security since 2008. His reporting won a 2005 honorable mention for Best Energy Writing from the National Press Foundation and 2009 recognition from the Society of Environmental Journalists. From 1997-2003, Clayton was the Monitor's higher education reporter exploring the basis for steep tuition increases and the black box of the Ivy League admissions process. He was co-winner

of several staff education-writing awards and, in 2002, won the Iris Molotsky Award for Investigative Reporting in Higher Education from the American Association of University Professors for his two-part series revealing affirmative action for men in the college admissions process. Clayton served as the Monitor's Toronto bureau chief from 1993-2007, reporting on Canadian culture and political affairs, including that nation's close call with Quebec secession.

Even The Department Of Homeland Security Wants You To Disable Your Java

Source: http://gizmodo.com/5975415/even-the-department-of-homeland-security-wants-you-to-disable-your-java

We've been concerned about the security of Java for a while now. There was that vulnerability that affected like a billion computers, and Apple went so far as to remove Java plugins from all OSX browsers. Now even the Department of Homeland Security is in on the act with a special message: "Yo, shut off that Java jazz".

The Java exploits can make your computer (Mac or PC) vulnerable to all kinds of nasty stuff from ransomeware to assorted other virus-y goodness. There are plenty of "exploit kits" out there to help script kiddies get their jollies by messing with your stuff. As such, the Department of Homeland Security's Emergency Readiness Team put out a notice saying "Due to the number and severity of this and prior Java vulnerabilities, it is recommended that Java be disabled temporarily in web browsers."

Oracle plans to release a patch on Tuesday that will fix the bulk of the problems by closing up a whopping 86 vulnerabilities, meaning that for the time being, you've got at least 86 vulnerabilities to worry about if you've got Java on. In the meantime, you best disable that stuff.

Grammar rules undermine security of long computer passwords

Source: http://www.homelandsecuritynewswire.com/dr20130125-grammar-rules-undermine-security-of-long-computer-passwords

When writing or speaking, good grammar helps people make themselves be understood. When used to concoct a long computer password, however, grammar — good or bad — provides crucial hints that can help someone crack that password, researchers at Carnegie Mellon University have demonstrated.

A team led by Ashwini Rao, a software engineering Ph.D. student in the Institute for Software Research, developed a password-cracking algorithm that took into account grammar and tested it against 1,434 passwords containing sixteen or more characters. A Carnegie Mellon University release reports that the grammar-aware cracker surpassed other state-of-the-art password crackers when passwords had grammatical structures, with 10 percent of the dataset cracked exclusively by the team's algorithm.

"We should not blindly rely on the number of words or characters in a password as a measure of its security," Rao concluded. She will present the findings on 20 February at the Association for Computing Machinery's Conference on Data and Application Security and Privacy (CODASPY 2013) in San Antonio, Texas.

Basing a password on a phrase or short sentence makes it easier for a user to remember, but the grammatical structure dramatically narrows the possible combinations and sequences of words, she noted.

Likewise, grammar, whether good or bad, necessitates using different parts of speech — nouns, verbs, adjectives, pronouns — that also can undermine security. This is because pronouns are far fewer in number than verbs, verbs fewer than adjectives and adjectives fewer than nouns. So a password composed of "pronoun-verb-adjective-noun," such as "Shehave3cats" is inherently easier to decode than "Andyhave3cats," which follows "noun-verb-adjective-noun." A password that incorporated more nouns would be even more secure.

"I've seen password policies that say, 'Use five words,'" Rao said. "Well, if four of those words are pronouns, they don't add much security."

For instance, the team found that the five-word passphrase "Th3r3 can only b3 #1!" was easier to guess than the three-word passphrase "Hammered asinine requirements." Neither the number of words nor the number of characters determined password strength when grammar was involved. The researchers calculated that "My passw0rd is $uper str0ng!" is 100 times stronger as a passphrase than "Superman is $uper str0ng!," which in turn is 10,000 times stronger than "Th3r3 can only b3 #1!"

The release notes that the research was an outgrowth of a class project for a masters-level course at CMU, Rao said. She and Gananand Kini, a fellow CMU graduate student, and Birendra Jha, a Ph.D. student at MIT, built their password cracker by building a dictionary for each part of speech and identifying a set of grammatical sequences, such as "determiner-adjective-noun" and "noun-verb-adjective-adverb," that might be used to generate passphrases.

Rao said the grammar-aware password cracker was intended only as a proof of concept and no attempt has been made to optimize its performance. But it is only a matter of time before someone does, she predicted.

European Union (EU) Issues a New Cybersecurity Strategy

Source: http://www.homelandsecurity.org/node/724

On February 7, the European Commission issued its first comprehensive strategy to prevent and respond to cyber disruptions and attacks. The new cybersecurity strategy, along with a proposal on network and information security,

aims to prevent and fight cybercrime, strengthen the security and resilience of networks and information security systems, and establish a more coherent European cyber security policy.

challenge, which the EU will address together with the relevant international partners and organisations, the private sector, and civil society.

EU High Representative Catherine Ashton said

The strategy is offering clear priorities for the EU international cyberspace policy:

- Freedom and openness: The strategy will outline the vision and principles on applying the EU core values and fundamental rights in cyberspace.
- The laws, norms, and EU's core values apply as much in the cyberspace as in the physical world: The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments.
- Developing cyber security capacity building: The EU will engage with international partners and organisations, the private sector, and civil society to support global capacity building in third countries. It will include improving access to information and to an open Internet, and preventing cyber threats.
- Fostering international cooperation in cyberspace issues: To preserve open, free, and secure cyberspace is a global

at the announcement of the new strategy: "For cyberspace to remain open and free, the same norms, principles, and values that we [EU] uphold offline must also apply online." Neelie Kroes, vice president of the European Commission responsible for the Digital Agenda said, "We are all here because we recognise the Internet is important: for our economy, for our values, and for our human rights. We all recognise that insecure systems could harm those benefits. And we recognise that we need to work together, within the EU and internationally, to achieve a safe and free Internet."

"The international dimension also features prominently with the objective of establishing a coherent international cyberspace policy. At the bilateral level, the new strategy underscores that cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-U.S. Working Group of Cybersecurity and Cybercrime.

EU Cyber Security Strategy – open, safe and secure

Source: http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm

A free and open Internet is at the heart of the new Cyber Security Strategy by the High Representative Catherine Ashton and the European Commission. The new Communication is the first comprehensive policy document that the European Union has produced in this area. It comprises internal market, justice and home affairs and the foreign policy aspects of cyberspace issues.

The Strategy is accompanied by a legislative proposal (a Directive) from the European Commission to strengthen the security of information systems in the EU. This would encourage economic growth as people's confidence in buying goods online and using the Internet would be strengthened.

The Strategy is offering clear priorities for the EU international cyberspace policy:

- Freedom and openness: The Strategy outlines the vision and principles on applying the EU core values and fundamental rights in cyberspace. Human Rights should also apply online and we will promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should promote democratic reform worldwide. The EU believes that increased global connectivity should not be accompanied by censorship or mass surveillance.
- The laws, norms and EU core values apply as much in the cyberspace as in the physical world: The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments.
- Developing cyber security capacity building: The EU will engage with international partners and organisations, the private sector and civil society to support global capacity building in third countries. It will include improving access to information and to an open Internet and preventing cyber threats.
- Fostering international cooperation in cyberspace issues: To preserve open, free and secure cyberspace is a global challenge, which the EU will address together with the relevant international partners and organisations, the private sector and civil society.

FAQ's on the International aspects of the Cyber Security Strategy

How can the core values be ensured in the worldwide web?

One example is human rights, which should also apply online as the European Union will promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform worldwide. The EU believes that increased global connectivity should not be accompanied by censorship or mass surveillance.

What EU norms and laws should be used in cyberspace?

The responsibility for a more secure cyberspace lies with all players of the global information society, from people to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. An important pre-condition for free and open Internet that brings political and economic benefits to societies worldwide, is to maintain a multi-stakeholder governance model of the Internet.

Will there be new laws to address cyber threats?

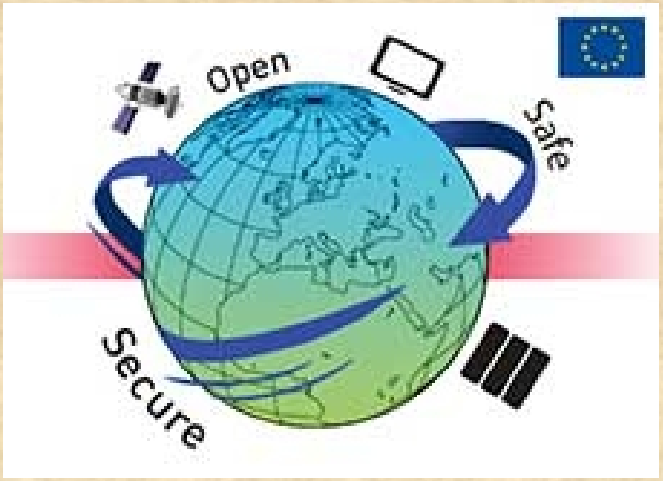
No, the EU believes we have many international law instruments already that should be applied in cyberspace. However, some governments have proposed new treaties and conventions in cyber issues that the EU cannot support. We fear that the argument of cyber security will be used as a pretext to justify limiting the freedom of expression and access to information. For instance, the Budapest Convention includes all the important elements to assist in investigation, prosecution, and international cooperation to address cybercrime.

At present 49 countries have signed the Convention and many countries outside Europe have introduced its principles into their legislation. The EU has assisted the Council of Europe in disseminating the principles of this Convention worldwide, and we are currently financing new programs to promote the Budapest Convention and increase the rule of law in this area.

What does the EU intend to do on capacity building?

The EU will engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries. It will include improving access to information and to an open Internet and preventing cyber threats. The EU will also actively participate in developing donor coordination for

helping capacity-building efforts. These actions will focus on enhancing criminal justice capabilities in training prosecutors and judges, and introducing the Budapest Convention



(Cybercrime Convention) principles in recipient countries' legal framework, building law enforcement capacity to advance cybercrime investigations and assisting countries to address cyber incidents.

How does the Strategy contribute to international cooperation in cyberspace?

To preserve an open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society. The EU will place a renewed emphasis on dialogue with third countries and international organisations, with a special focus on like-minded partners that share EU values. At bilateral level, cooperation with the United States is particularly important and will be further developed.

What the EU is doing on cyber defence issues?

Within the Common Security and Defence Policy, the European Defence Agency (EDA) is developing cyber defence capabilities and technologies, improving cyber defence training & exercises. Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, the private sector and academia in the EU.

The EU is also promoting early involvement of industry and academia in developing solutions and in strengthening Europe's defence industrial base and associated R&D innovations in both civilian and military organisations. The EDA will promote civil-military dialogue and contribute to the coordination between all actors at EU level – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment and establishing a cyber-security culture.

Why does the Strategy address civilian and military issues?

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, the private sector and academia in the EU. To avoid duplication, the Union will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

Are the EU and NATO cooperating in cyber security?

There is a regular cooperation going on between the experts. After the Strategy is adopted, we intend to intensify cooperation with NATO in cyber security. Dialogue with NATO should ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

Next Steps

The Directive must pass through the Council of Ministers and the European Parliament before adoption whilst the Cyber Security Strategy will remain as it is as it is not legislation.

Emiratis train with the best to foil cyber threat

Source: http://www.thenational.ae/news/uae-news/technology/emiratis-train-with-the-best-to-foil-cyber-threat

BAE Systems Detica, an international business and technology consulting company specialising in collecting, managing and exploiting information to reveal actionable intelligence, will be training Emiratis at their Cyber Threat Centre in the UK, said Tim Wood, Detica's Middle East director.

"A lot of what we do is try to work with partners and local organisations to take this cutting-edge technology and adapt it to their needs here in the UAE," said Mr Wood.

"We are going to have UAE nationals at our Cyber Security Threat Centre, working side by side with our cyber analysts."

Mr Wood added that the team, which he did not name, will be working on identifying targeted

cyber attacks and dealing with them.

"The centre essentially provides security and end-to-end support to large multinational organisations where we have the capability to identify advanced and targeted threats," he said at Idex yesterday.

It also provides a specialist response unit that, after identifying the attack, deals with the hardware that has been compromised and maintains the integrity of the system.

According to Mr Wood, government organisations as well as defence and aerospace corporations are facing a growing threat of targeted cyber attacks that are designed to conduct a specific malicious activity.

"In 2012, we had 240 cases of targeted cyber attacks," he said, 24 of which were in the Arabian Gulf. "Out of these attacks, the vast majority are espionage attacks, where sensitive data is being targeted for theft," he said.

The majority of these attacks were state sponsored, he added, with most of them originating in China. "We are now monitoring over 20 attack groups and they are from China, with a few based out of the Middle East and Eastern Europe."

According to Dan Jeffery, head of the commercial sector at Detica, the targeted attacks usually centre on industrial control systems that can present a risk to not only machinery and hardware but human life.

"In June 2010, the Stuxnet virus shut down centrifuges at Iran's Natanz uranium enrichment plant. They controlled the centrifuges and broke them down," he said.

"An attack can target an oil plant and open and close valves, causing pressure to build up and then creating an explosion. Such viruses also delete themselves and become untraceable."

The viruses, also known as malware, are designed to steal secrets, wipe data, shut down corporate computers and even sabotage nuclear power plants.

Last year, the Mahdi Trojan affected the UAE. The virus records keystrokes, screenshots and audio and steals text and image files. It has infected computers primarily in Iran, Israel, Afghanistan, the UAE and Saudi Arabia, including systems used by critical infrastructure companies, government embassies and financial services firms.

Other target industries include banking, legal and energy.

"Law firms have patent information, merger and acquisition records and personal information of important people - they are regular targets for attack," Mr Jeffery said.

Detica uses a system that analyses the behaviour of the attack group and the cyber threats in a bid to pre-empt them or reduce their effect.

"We get real-time alerts and respond to it immediately," Mr Wood said. "The problem with cyber security is that more and more people are creating new threats every day and we have to keep following the trends and their development."

Mr Jeffery added: "What is needed is to keep feeding the manpower in the cybersecurity field by educating more Emiratis in it to keep track of this rapidly growing and evolving threat."

Chinese Hackers Have A Weapon Of Mass Destruction That No One Is Talking About

Source: http://www.businessinsider.com/mandiant-china-hackers-wmd-no-one-mentions-2013-2

The Grid

The rousing report out of Mandiant about Chinese internet exploitation focused primarily on the widespread, systematic, state-sponsored thievery of proprietary data.

What it also mentioned (almost in passing) was the penetration of American energy structures, what most people call "critical infrastructure." Exploiting the aging electrical grid, in a cyber-military strike, has been a growing concern of planners in the U.S. Government.

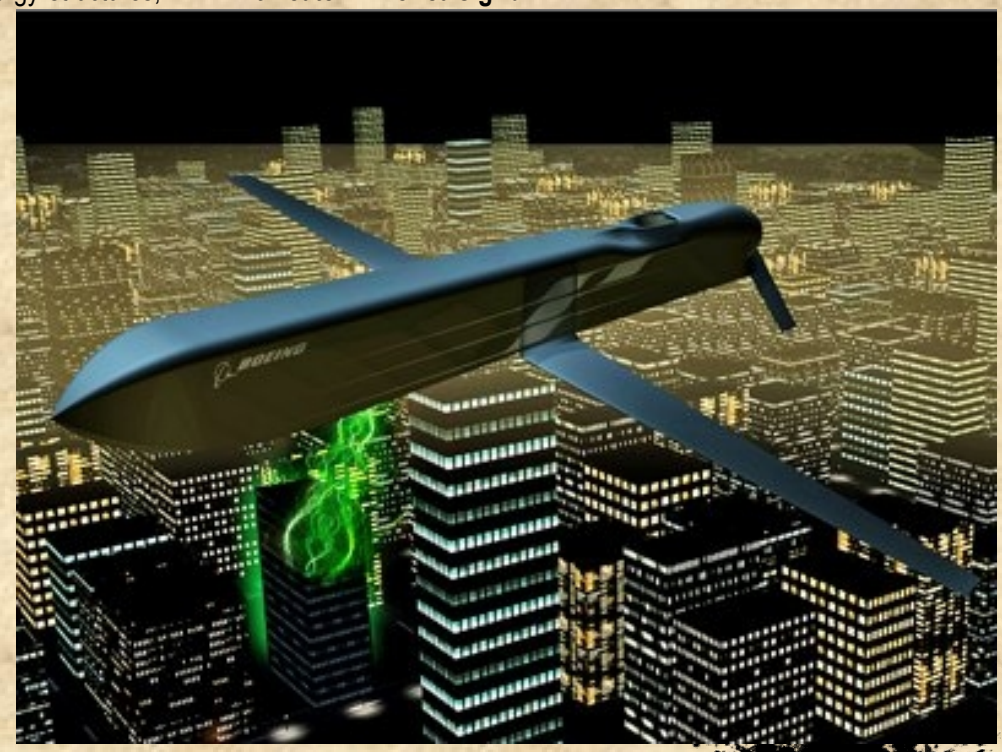
Yet hackers don't normally headline talk of aging grids.

Usually talk of electrical Weapons of Mass Destruction is accompanied with conjecture about space-bound nuclear bombs and their theoretical electromagnetic pulse (EMP) — a shockwave that knocks out circuits, transformers and just about anything requiring electricity.

Newt Gingrich's grave EMP assertions during the Republican primaries (famously couched with punchlines about "Moon bases") immediately met with criticism from experts in the defense community. Such a projectile would be detected and shot out of the air, or space, they said.

Late last year we covered how Boeing had developed an EMP missile, capable of flying over a city and permanently zapping its electrical structure. While **that might not be the most likely candidate** for an assault on the American grid, **it further legitimized electrical grids as potential targets.**

It seemed like loss of proprietary, corporate information trumped the news headlines, but the Mandiant report also showed that **it's not EMPs which truly threaten America's grid.**



It's software exploits, particularly from the Chinese military.
A Department of Homeland Security official told the WSJ in 2010 that network inspections had "found software tools left behind that could be used to destroy infrastructure components," following hacks from

Russia and China

Russia and China of course denied the reports. "It's like (improvised explosive devices) in Iraq.

Bomb makers have certain signatures, and looking at a bomb, you can tell who and where that signature comes from," said David Lacquement, a cyber security expert with Science Applications International Corporation, and formerly the Army general in charge of operations for U.S. Cyber Command.
Lacquement said that the ability to execute 'kinetic' cyber operations to destroy real world targets is already well established (See also: Stuxnet). Experts say syncing those actions up with other external forces — an invading army, or more likely, a hurricane — would have catastrophic effects.
"These (cyber capabilities) are not in the realm of make believe, they are reality," said Lacquement.

The Northeast Blackout of 2003 was the result of a "software glitch" — essentially a bug in the system — that sent a 3,500 MW power surge out into the grid. Synchronizing many of those together, along several power hubs down the East Coast, would initially cause untold damage.
Even without a hurricane or an earthquake, the following long-term effects would be something akin to a Weapon of Mass Destruction — at least the Air Force and Leon Panetta think so.
A 2010 report out of North American Electric Reliability Program listed 'cyber attacks' right along with nuclear explosions as a massive threat to existing structures.
From the report:
"The physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale, as could be effected by any of these threats, **could result in prolonged outages as procurement cycles for these components range from months to years."**
Imagine the effects of Hurricane Sandy carried out into the realm of months instead of weeks — the result is apocalyptic. Loss of water pressure followed closely by total loss of water, loss of heat or air conditioning, spoiled food, and then in only a matter of time, little or no access to gasoline — these things conjure

images better associated with the '80s flick "Mad Max" than with reality.

Jack Lind

President Obama recently announced a new public/private information sharing initiative, though it was barely audible above the deafening sound of Marco Rubio reaching for a water bottle.

If Americans don't want to be fighting over water bottles though, action is needed to avoid catastrophe. Hopefully Mandiant's report will act as a loudspeaker, turning Team Obama's cyber security squeak into a shout, and opening the doors for more public conversation about these threats.