# Διαφάνεια7.JPG

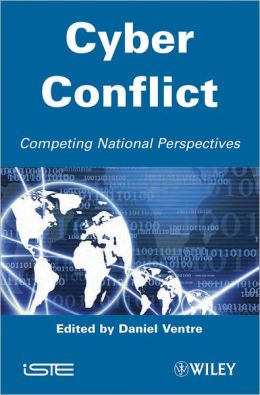
# G:\Staff for NSL\Λεζάντες NSL\Slide5.JPG

# BOOK: Cyber Conflict - Competing National Perspectives

**Edited by Daniel Ventre, CNRS, France**

Publication Date: April 2012   Hardback   352 pp.

Source: http://www.iste.co.uk/index.php?f=x&ACTION=View&id=484

Today, cyber security, cyber defense, information warfare and cyber warfare issues are among the most relevant topics both at the national and international level. All the major states of the world are facing cyber threats and trying to understand how cyberspace could be used to increase power. Through an empirical, conceptual and theoretical approach, Cyber Conflict has been written by researchers and experts in the fields of cyber security, cyber defense and information warfare. It aims to analyze the processes of information warfare and cyber warfare through historical, operational and strategic perspectives of cyber attack. It is original in its delivery because of its multidisciplinary approach within an international framework, with studies dedicated to different states – Canada, Cuba, France, Greece, Italy, Japan, Singapore, Slovenia and South Africa – describing the state’s application of information warfare principles both in terms of global development and “local” usage and examples.

**Contents**

1. Canada’s Cyber Security Policy: A Tortuous Path Toward a Cyber Security Strategy, Hugo Loiseau and Lina Lemay.  
2. Cuba: Towards an Active Cyber-defense, Daniel Ventre.  
3. French Perspectives on Cyber-conflict, Daniel Ventre.  
4. Digital Sparta: Information Operations and Cyber-warfare in Greece, Joseph Fitsanakis.  
5. Moving Toward an Italian Cyber Defense and Security Strategy, Stefania Ducci.  
6. Cyberspace in Japan’s New Defense Strategy, Daniel Ventre.  
7. Singapore’s Encounter with Information Warfare: Filtering Electronic Globalization and Military Enhancements, Alan Chong.  
8. A Slovenian Perspective on Cyber Warfare, Gorazd Praprotnik, Iztok Podbregar, Igor Bernik and Bojan Ticar.  
9. A South African Perspective on Information Warfare and Cyber Warfare, Brett van Niekerk and Manoj Maharaj.  
10. Conclusion, Daniel Ventre.

***Daniel Ventre*** *is an engineer at CNRS, a researcher with CESDIP (Centre for Sociological research on the Law and penal institutions), in charge of Télécom ParisTech and the ESSEC Business School and General Secretary of GERN. He is the author of a number of books and articles on cyberwarfare, information warfare, cyberconflict, cybersecurity and cyberdefense.*

The history of cyber attacks – A timeline

Source: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

**1988**

The Morris worm - one of the first recognised worms to affect the world's nascent cyber infrastructure - spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted under the the US' computer fraud and abuse act. He now works as a professor at MIT.

**DECEMBER 2006**

**NASA was forced to block emails with attachments** before shuttle launches out of fear they would be hacked.

Business Week reported that the **plans for the latest US space launch vehicles** were obtained by unknown foreign intruders.

APRIL 2007

Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted.

The attacks were more like cyber riots than crippling attacks, and the Estonians responded well, relaunching some services within hours or - at most - days.

**JUNE 2007**

The US Secretary of Defense’s unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks.

**OCTOBER 2007**

China’s Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas.

In 2006, when the China Aerospace Science & Industry Corporation (CASIC) intranet network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

**SUMMER 2008**

The **databases of both Republican and Democratic presidential campaigns were hacked** and downloaded by unknown foreign intruders.

**AUGUST 2008**

Computer networks in **Georgia** were hacked by unknown foreign intruders around the time that the country was in conflict with Russia. Graffiti appeared on Georgian government websites.

There was little or no disruption of services but the hacks did put **political pressure on the Georgian government** and appeared to be coordinated with Russian military actions.

**JANUARY 2009**

Hackers attacked **Israel’s internet infrastructure** during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers.

Israeli officials believed the attack was carried out by a criminal organisation based in a former Soviet state, and paid for by Hamas or Hezbollah.

**JANUARY 2010**

A group named the "**Iranian Cyber Army**” disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message.

The same “Iranian Cyber Army” had hacked into Twitter the previous December, with a similar message.

**OCTOBER 2010**

Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programme.

**JANUARY 2011**

The **Canadian government reported a major cyber attack against its agencies**, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence.

The attack forced the Finance Department and Treasury Board, Canada’s main economic agencies, to disconnect from the Internet.

**JULY 2011**

In a speech unveiling the Department of Defense’s cyber strategy, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.

**OCTOBER 2012**

**The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed “Red October,” that had been operating since at least 2007.**

**Hackers gathered information through vulnerabilities in Microsoft’s Word and Excel programmes. The primary targets of the attack appear to be countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well.**

**The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.**

**MARCH 2013**

South Korean financial institutions as well as the Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea.

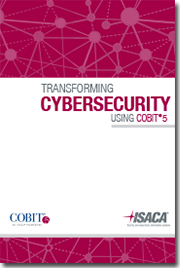
## New guide highlights three cyber security game changers

Source: http://www.homelandsecuritynewswire.com/dr20130625-new-guide-highlights-three-cyber-security-game-changers

Cybercrime is on the rise, and it will grow even faster if organizations ignore an emerging group of cybersecurity game changers: always-on connectivity, an increasingly IT-centric society, and a new class system that separates people by technology skills.

The Information Systems Audit and Control Association’s (ISACA)s latest guide, Transforming Cybersecurity Using COBIT 5, examines the impact of these game changers and how to manage and transform security by using COBIT 5, a business framework for the governance and management of enterprise information and technology. Along with publication of the guide, IT association ISACA also announced the formation of a global cyber security task force.

ISACA says that the three game changers named in the guide provide both motive and opportunity for cybersecurity breaches and criminal activities — especially the advanced persistent threat (APT) — if ignored.

“In just the past three years, the number of threats and vulnerabilities has grown almost exponentially. By using COBIT 5, security professionals have a systematic approach for overcoming some of their biggest internal barriers — especially inadequate budget and lack of senior management support,” said Rolf von Roessing, lead developer of the guide and president of FORFA AG.

This latest addition to ISACA’s cyber security series is designed for information security managers, corporate security managers, end-users, service providers, IT administrators, and IT auditors. It includes guidance on using the COBIT 5 framework to integrate cyber security with an overall approach to security governance, risk management and compliance, as well as eight principles for transforming security.

“The enormous opportunities inherent with cloud, mobility, social networking and big data also create significant security risks, and most organizations are ill-prepared to respond effectively. If we want to defend ourselves from sophisticated and targeted cyberattacks, it’s time to shift the industry’s thinking from a focus on compliance and perimeter security to a more proactive posture that is all about protecting the crown jewels,” said Eddie Schwartz, chair of ISACA’s Cybersecurity Task Force and chief information security officer (CISO) at RSA, The Security Division of EMC.

A recent ISACA cyber security survey of more than 1,500 security professionals worldwide found that 94 percent of respondents believe the APT represents a credible threat to national security and economic stability. Top risks were seen as loss of enterprise intellectual property (26 percent), loss of customer or employee personally identifiable information (24percent), and damage to corporate reputation (21 percent).

# New Cybersecurity Threats Target Medical Devices

Source: http://au.businessinsider.com/new-cybersecurity-threats-target-medical-devices-2013-6

Getty/ MCT



A new threat has got the attention of cybersecurity monitors after US security experts say the hacking of devices such as pacemakers and insulin pumps is possible.

Sky News has reported the US Food and Drug Administration is warning manufacturers to step up their vigilance, saying ‘cybersecurity vulnerabilities and incidents could directly impact medical devices or hospital network operations’.

No deliberate hacking of medical devices has yet to be reported according to officials.

Kevin Fu, professor at the University of Michigan, co-wrote a 2008 research paper which focused on the risks of implantable devices and how they could be re-programmed by hackers.

“It takes just a blink of the eye for malware to get in” says Fu.

Regulators have also suggested hospital equipment such as monitoring systems, scanners and radiation equipment are connected to networks which could potentially experience similar security breaches, reported Sky.

“The vast majority of medical devices in hospitals I’ve been to use Windows XP or Windows 95. These are extremely vulnerable to computer malware,” Fu said.

In light of the new findings US Department of Homeland Security’s Cyber Emergency Response Team for industrial systems has said security should be stepped up for surgical devices, ventilators, drug infusion pumps and other equipment.

While the issue is now on the cybersecurity lookout experts say despite the risks, people still are better off with these devices than without.

# Cyber-retaliation: How security is becoming a priority for the Middle East

**By Robert Jones**

Source: http://www.zdnet.com/cyber-retaliation-how-security-is-becoming-a-priority-for-the-middle-east-7000017197/

Kevin Mitnick was in town recently For anyone who doesn't know the name, in the mid-1990s, Mitnick was the most-wanted and best-known hacker in the world.

Back in 1995, it was not just the world's computer press that covered his story. The daily newspapers realised they had a new antihero to tear into, warning the public of the dire threats we faced of a hacking epidemic. Thanks to Mitnick and his prison sentence, hacking exploded into the conscience of the general public.

Now a world-famous former hacker and renowned security expert, he flew in to Dubai to speak at the Gulf Information Security Expo & Conference. Although hacking is infrequently reported in the Middle East, IT security is big business, with all the major software houses having offices in the region. Instances of cyberattacks are on the rise, becoming more sophisticated and, in some cases, having political ramifications seen around the world.

Mitnick's timing was perfect of course, because two days before his arrival, the Virgin Radio website in Dubai was hacked, in protest at the growing international celebrity culture of the UAE. Although Arabic music in the UAE is popular, with so many expats living in the country Abu Dhabi and Dubai have become mainstay slots in bands' international tours, with artists such as the Stone Roses, Metallica, Bruno Mars, Guns n' Roses and Kanye West  having played here so far this year.

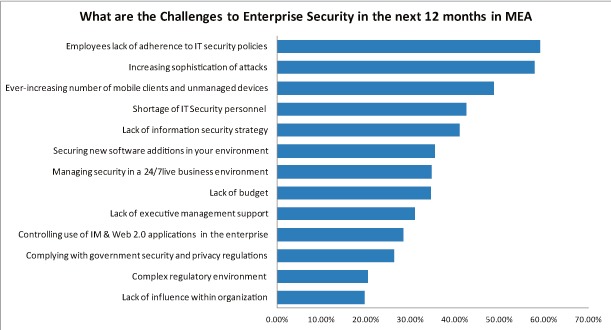
According to UAE newspaper The National, the Emirati hacker, calling himself OxAlien, was angry at the number of western bands playing — usually to packed crowds — in the UAE. He left a message on Virgin's site claiming: "Your database is with me. I'll sell the admin login script in the black market to get some cash. No files have been deleted from your server."

Mitnick's message to delegates at the conference was that hackers are increasingly using social engineering techniques to find and then attack weaknesses in companies' security — a technique he mastered as a teenager. Describing it as a low-risk, cheap and high-return method of attack, he told the audience that no software security can protect against such methods, because social engineers exploit human nature.

In April, the analyst group IDC reported that in the Middle East, a lack of adherence to IT security policies by employees was the number one challenge faced by IT professionals, followed by the threat of increasingly sophisticated attacks. The analysts said that with the combined growth of mobile devices used in the workplace that require securing, the increasing sophistication of threats and the (albeit it slow when compared to Europe and the US) growth of cloud services, organisations in the region are beginning to change their security strategy, turning to managed security services.

The amount of money spent on IT security is growing at 15 percent a year, IDC said, and in some cases, companies are spending big to protect their networks. Last year, MEED reported that the major national oil companies in the Middle East spend around $10m annually to secure their systems.

Security is high on the minds of IT professionals in the region and attitudes are hardening. When I first got to the Middle East, I never got the feeling that external attacks were considered a major threat to businesses based here in the same way that it is in other regions.

Hacking of the sort suffered by Virgin Radio may be unusual here, but is not unique. In mid-May, Saudi Arabia admitted that some of its government websites had come under a sustained denial of service attack, with a group called Saudi Anonymous using Twitter to not just claim responsibility but also provide a running commentary of its actions and targets in both Arabic and English, finally declaring on 18 May that: "Today is our last day on #OpSaudi, moi.gov.sa [Ministry of Interior] will be our last target."

The group used the hastag OpSaudi as it updated on the attacks. It put out the cryptic message #OPpetrol, with a message on 13 June saying simply "1 week". If an attack had been slated to start on 20 June, the world's hydrocarbons companies would have had plenty of warning to prepare.

But while the attacks on Virgin Radio and Saudi government sites are a malicious inconvenience, the big threat now is around the major industries of the Middle East. This was brought home a couple of years ago, when the IT systems in Iran's two nuclear power plants were attacked.

The Bushehr nuclear facility, central to the worldwide sanctions that have been imposed on Iran, was hit by Stuxnet. Discovered in June 2010, the malware was designed to attack control systems and in particular Siemens' program logic controllers used in industrial facilities to manage parts such as control pumps and pressure gauges. Once Stuxnet was introduced to Iran's nuclear power plants, it is believed by USB in 2009, it allowed the attacker to sabotage the control systems.

The attack, blamed on the US and Israel, damaged both Iran's centrifuges and its nuclear ambitions, delaying the opening of the plant. But it also brought home to organisations in the Middle East that cyberattacks were a real threat, it highlighted the importance of strong security systems and caused some internal soul searching. If Iran's nuclear facilities can be hit, then could the same happen to the region's oil and gas facilities, so important to the economies of the oil-exporting nations, or the power and water desalination plants?

And of course it did. In August 2012, the national oil and gas company of Saudi Arabia, Saudi Aramco, was hit. One of the world's most valuable companies, at an estimated $10 trillion, and the world's biggest oil producer, pumping about 12.5 million barrels a day from its fields, Aramco was hit by a malware attack that infected 30,000 computers. This was swiftly followed by a similar attack on RasGas in Qatar.

Like Aramco, RasGas, which is 70 percent owned by government entity Qatar Petroleum, said that its operations were not impacted by the attack. But as the world's second largest producer of liquefied natural gas, at about 36 million tonnes a year, any impact on its production would have hurt countries around the globe. Its exports go to South Korea, India, Belgium, and Holland, among others. The UK is also reliant on RasGas, with tankers delivering LNG to its three main gasification terminals of South Hook, Dragon and Isle of Grain. Iran was blamed in both cases, although there has been no official confirmation that its government was behind the attacks.

Now, security experts elsewhere are warning that the instances of attacks emanating from the Middle East is rising fast, with around 10 US utility companies the target of attempts to take over plant processes (sound familiar?). So far, no group or country has been blamed but the US Department of Homeland Security has put companies on alert.  And it is difficult not to allow the thought to float across your mind that this just might be a dangerous game of cyber retaliation.

***Robert Jones*** *and his family have lived in Dubai since 2007 and he has since travelled extensively around the region. He is head of content development for MEED, a leading business intelligence service covering major Middle East infrastructure projects and economies.*

**Britain 'under attack' in cyberspace**

**By Gordon Corera** (Security correspondent, BBC News)

Source: http://www.bbc.co.uk/news/uk-23098867

Britain is seeing about 70 sophisticated cyber espionage operations a month against government or industry networks, British intelligence has told the BBC.

GCHQ director Sir Iain Lobban said business secrets were being stolen on an "industrial scale".

Foreign hackers have penetrated some firms for up to two years, he said.

And he denied that his organisation had broken the law in receiving information from the Prism spy programme.

Sir Iain told BBC Radio 4: "People are going after intellectual property and then seeking to translate it into national gain.

"We started a couple of years ago thinking this was going to be very much about the defence sector but really it's any intellectual property that can be harvested."

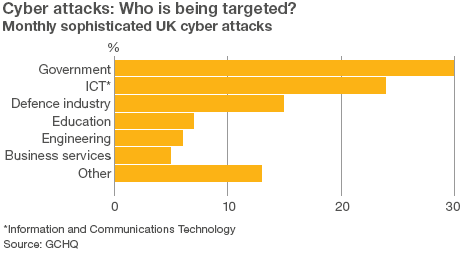
Foreign intelligence services are behind many of these attacks, according to Britain's Security Service MI5.

British businesses are waking up the threat of cyber espionage. Sir Michael Rake, chairman of BT and president of business lobby group CBI, has been warning fellow businessmen about the dangers. "These threats are real, they're sophisticated, they do financial and reputational damage," he told the BBC.

"There's been a lot of concern around espionage in gaining information of advanced planning and design and it is critical because one of our big strengths in the UK is our design capabilities," he added.

The job of the Security Service MI5 involves dealing not just with terrorist threats but also cyber attacks.

"There are now three certainties in life - there's death, there's taxes and there's a foreign intelligence service on your system," explained MI5's head of cyber (who asked not to be named), in his first public interview inside MI5's Thames House headquarters.

MI5's origins are as a counter-espionage agency - catching foreign spies - and that is still what it tries to do in cyberspace.

"There are hostile foreign states out there who are interested in a company's mergers and acquisitions activity, their joint venture intentions, their strategic direction over the next few years and that information would be valuable to that country's state owned enterprises," he said.

So who is behind these attacks? Both MI5 and GCHQ said they knew who was behind the attacks but neither was willing to say.

"We're sure we know who it is," argued Sir Iain, saying only that in many cases attacks are "state sponsored".

"Attribution can be very hard and it's very difficult to do attribution in real time but over a period you can build up a pretty strong idea," he explained.

**'Political game'**

Foreign Secretary William Hague also declined to point the finger now but did not rule out doing so in the future. "That's not been our approach so far. But that might have to change if things get worse," he told the BBC.

Washington has taken a different approach. Both the administration and Congress are explicit about what they see happening to American companies.

"Blueprints for their products that make them successful are being stolen at a breath-taking pace, taken back to China, repurposed and then they re-engineer it and then compete against those companies with those products which they've stolen," Congressman Mike Rogers, chairman of the House Intelligence Committee told the BBC.

"I stand back in awe as a professional at the breadth, depth, sophistication and persistence of the Chinese espionage effort against the United States of America," Michael Hayden, former director of America's spy agency the NSA said.

That is, of course, a slightly disingenuous answer since most experts believe that the NSA (along with GCHQ) is amongst the most adept and busy of all global spy agencies when it comes to stealing the secrets of other countries.

Hayden however draws a distinction. "We steal secrets too… but we steal only those things that keep British or American subjects safe and free. We don't steal things to make Americans - or in GCHQ's case British - subjects rich. The Chinese do."

The view from Beijing is very different. It sees America using the charge of economic espionage to distract from its own aggressive cyber activities - ranging from traditional espionage to preparing for cyberwar.

The Chinese Foreign Ministry invited me in to talk to the country's lead negotiator on cyber issues. "China is one of those countries suffering most by hacker attacks," Dr Huang Huikang argued. "They are misunderstanding what happened in China and sometimes we think this is a political game. It's not true and not fair to China."

China is watching the Pentagon grow its cyber command five-fold to nearly 5,000 personnel and also worries at the way in which American corporations still play a dominant role in the internet globally.

"Getting hold of technological secrets so that you can learn from another country is nothing new," says Professor Xu Guangyu, a former general in the People's Liberation Army. "It happened well before the advent of cyberspace. The main thing is that the control of cyberspace is too concentrated in the hands of the United States."

China's argument has been bolstered by Edward Snowden's leaked documents which portray a huge level of espionage against Chinese (and other) computer networks and information flows.

The interview with GCHQ's director was conducted before Snowden's documents began to emerge. A number of his revelations concerned the work of GCHQ including its receipt of information from major technology companies through America's Prism programme.

In a statement after the revelations, Sir Iain said that GCHQ did not circumvent the law and worked under a robust framework. "I can say that any data obtained by us from any other nation which involves individuals in the UK is subject to proper UK statutory controls and safeguards," he told the BBC.

"The secret intelligence provided by all the UK security and intelligence agencies is vital to defeating terrorism and maintaining Britain's broader national security. Acquiring it in ways that somehow evade UK law would be a contradiction in terms."

# Former police chief Bratton launches a social network for cops

Source:http://www.chicagotribune.com/news/sns-rt-us-usa-police-socialmedia-20130629,0,766964.story

Bill Bratton, the high-profile police commissioner who has run three of America's largest police forces, is preparing to launch the first comprehensive social media network for police officers - a kind of Facebook for cops.

The network, known as BlueLine, will be launched globally at the International Association of Police Chiefs annual conference in Philadelphia in October.

BlueLine is part of a growing trend in high-tech information-sharing among law enforcement agencies that proponents say is producing a force-multiplying effect on crime-fighting in an era of dwindling police budgets and manpower. The collaboration enables better communication between different jurisdictions and helps police identify patterns of criminality.

Combining the most popular user functions of a number of leading social media sites, BlueLine is being billed by Bratton as the first secure network for cops. It's also a safer alternative for a younger generation of officers who Bratton says share a shocking amount of information on public networks.

"If you're a SWAT officer, gives you the ability to find other SWAT officers in departments around the country and engage them, share best practices, talk about innovations," Bratton told Reuters recently.

The for-profit company behind BlueLine, Bratton Technologies, was founded to develop the proprietary product, and aims to generate revenue from a spectrum of cop-related products - everything "from socks to Glocks," said BT Chief Strategy Officer Jack Weiss.

The network is being beta-tested this summer among about 100 officers in the Los Angeles Police Department, Los Angeles Sheriff's Department and the University of Southern California police force.

Several dozen more police departments will join the beta test later this summer, said Bratton, who is BT's chief executive officer.

Most existing law enforcement information-sharing networks involve sharing intelligence about specific cases, while BlueLine is geared toward collaboration on policing issues like gangs or drugs and product and technology advances.

Bratton has led the New York, Los Angeles and Boston police departments and was responsible in 1995 for introducing Compstat - a groundbreaking software-driven, crime-fighting strategy that mapped crime patterns and enabled real-time deployment of forces. For him, "collaboration is the key to successful policing."

BlueLine includes the key elements and the look of Facebook, with "like" and "share" buttons and the ability to post messages, photos or video clips on a wall visible to other users.

The network also features secure videoconferencing capabilities and an iTunes-like app store open to third-party developers. A commercial component will allow companies that make policing products to market them directly to members of the roughly 18,000 state and local law enforcement agencies in the United States and beyond.

The startup is being funded by G2 Investment Group, said G2 Chief Executive Officer Todd Morley. Bratton declined to say how much capital was involved.

**Crowdsourcing Cop Communities**

Open only to accredited law enforcement officers, BlueLine users can create or join customized groups, with names like Gangs, Narcotics, New Technology or Sex Crimes - and then "crowdsource" colleagues for help with general aspects of investigations.

One group might discuss the benefits and drawbacks of a new type of police radio, or a new drug that has hit the streets of their town.

If a gangs investigator in one department comes across an unfamiliar tattoo on a suspected gang member, the cop can post it to a Gangs network, and someone from another department may help identify it as the sign of a new crew. Members can search for each other by name, geography, expertise and interest.

Data analytics companies are developing BlueLine applications, which will let users create databases - of gang tattoos or graffiti tags, for instance - and analyze them.

BlueLine will operate a secured network requiring multiple verifications to join, with protocols based on the FBI's Criminal Justice Information Services (CJIS) guidelines, established to ensure secure transmission of criminal case information online, said David Riker, president of Bratton Technologies.

"This is not intended to replace strategic police communications capabilities," said Bratton. "It is primarily for people to find each other," he said. "We are quite clear about the guardrails we are staying within."

# Webcam hacking exploits Chrome Inbuilt Flash player for Camjacking

Source:http://securityaffairs.co/wordpress/15402/hacking/webcam-hacking-exploits-chrome-flaw.htm l?goback=.gde\_4962526\_member\_254989352

Webcam hacking, hackers are increasing their interest on millions of cams that surround us. These prying eyes are everywhere, in the street as in our home, gaming consoles, smartTV and PC are all equipped with a camera.

The impressive diffusion of mobile devices equipped with web cameras makes Webcam hacking very attractive and it is considerably a serious menace for users’ privacy, these attacks are silenced and could cause serious problems. Think for an instant of the implication related to Webcam hacking made by cybercriminals or by a government for surveillance purpose, we have seen it in the movies but today it is a reality.

Let’s start from domestic webcam, the Webcam hacking is a reality according to a recent post published by Egor Homakov that highlighted a serious flaw in Google Chrome’s integrated Flash player.

Egor Homakov demonstrated that just pressing the play button a user could authorize an attacker to access his webcam giving him the possibility to capture video and audio without getting permission.

“*I’ve heard a hacker could access my webcam and watch me in front of my computer. Could this really happen?*“ YES, it is possible exploiting new Flash based flaw in Google Chrome.

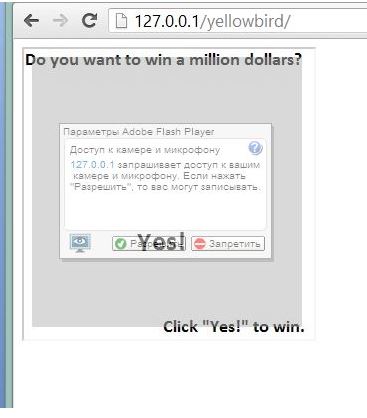
“*This works precisely like regular clickjacking – you click on a transparent flash object, it allows access to Camera/Audio channel. Voila, attacker sees and hears you,*” Homakov said.

*This type of attack dubbed is known for several years as Clickjacking, a known vulnerability in Adobe Flash Player Settings Manager.*

Adobe is aware of Clickjacking attacks and it resolved the flaw with a change to the Flash Player Settings Manager SWF file hosted on the Adobe website.

Differently for *Camjacking*attacker could hide the Flash Player security message when the flash file is trying to access a web camera or to a microphone.

According the researcher the Webcam hacking is possible exploiting an invisible Flash element present on the page, it is enough that victim using Chrome Browser clicks on it is.

*“That’s what I thought as well. written a simple page with the opacity and flash container (flash requested access to the web-camera), it was observed that 21 Firefox, Opera 12.15 or ignore transparency flash animation, or just do not handle. But IE and Chrome 27.0.1453.110 10 well treated transparency and allowed to place himself on top of the text and / or image. That, no doubt, would have gone into the hands of web designers. But to remain on its laurels were just not interested, and I started to dig deeper, taking the idea of Clickjacking attack, but to remake it to fit their needs, ie to borrow all the “useful” function for the attacker. I chose access to the webcam (of course, yet we can get access to the microphone, but it was important, then?) So, I wrote a simple USB flash drive, take a picture with the help of a web camera and sends it to the server. “*

Homakov verified that Webcam hacking with Camjacking doesn’t work with semi-transparent on IE.

An Adobe security team representative has confirmed the bug related only to Flash Player for Google Chrome.

Will Google solve the problem in the seven days established for fixing the bug to its products?

But the concerns do not stop at home webcam, Craig Heffner, a former software developer with the NSA declared to have discovered the previously unreported bugs in digital video surveillance equipment from firms including Cisco Systems Inc, D-Link Corp and TRENDnet.

“It’s a significant threat,”

“Somebody could potentially access a camera and view it. Or they could also use it as a pivot point, an initial foothold, to get into the network and start attacking internal systems.” said the specialist.

He announced his intention to demonstrate it during the next Black Hat hacking conference, on July in Las Vegas.

Heffner revealed that he has discovered hundreds of thousands of surveillance cameras exploitable by attackers via Internet.

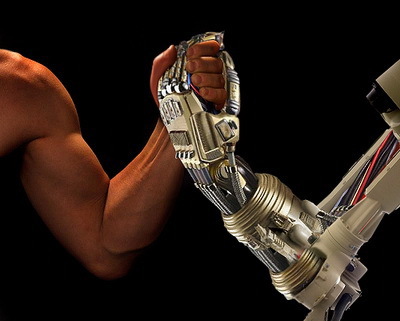
This is not a movie, neither an episode of the television serie Person of Interest … This is reality and maybe the Big Brother is already exploiting it!

**Our computers are not going to kill us all: Cyber-war is military fiction**

Source:http://www.theglobeandmail.com/commentary/cyberspace-is-not-a-combat-zone/article130355 62/

“The next Pearl Harbor we confront could very well be a cyberattack.” That’s what Leon Panetta, then head of the CIA, warned two years ago. A former U.S. director of national intelligence, Michael McConnell, warned in December of “the cyber equivalent of the collapse of the World Trade Centers.” Military organizations such as NATO want to devote considerable resources to cyberwarfare, and warn governments that they should spend far more on weapons of online war.

We tend to believe them. To those of us who grew up in the early decades of the Internet, reading William Gibson and watching Tron, the idea of a distinct and tangible “cyberspace,” as Mr. Gibson coined it, seems believable. If war is hell in meatspace, then imagine what it will be like when it moves into the online world, where all our communications and private data are stored, where the machines that control our entire lives can be hacked. If the Internet is everywhere, wouldn’t a cyberwar be a total war?

Once we started believing this, the whole world seemed to confirm it. An online virus was used by Israel and the United States to disable a uranium-enrichment facility in Iran. China uses a facility to steal data from the West. France, Britain and the United States, as we’ve recently learned, are mass-harvesting the online communications and phone calls of foreigners (and possibly their own citizens), and the man who revealed this, Edward Snowden, is in the midst of a globe-trotting flight across the settings of vintage James Bond movies. If this is what cyber cold war looks like, how horrid would real cyberwars be?

We can imagine them, and make movies about them, but the reality is far more mundane and less threatening.

That’s the conclusion made by Thomas Rid, an expert on cybersecurity and intelligence at the department of war studies at London’s King’s College. His forthcoming book’s straight-up title, Cyber War Will Not Take Place, is a call for sanity: There is no distinct “online world,” and the many forms of online crime and mischief are not a threat to our existence or our civilization.

“Cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future,” Mr. Rid writes.

Instead, he says, “the opposite is taking place: a computer-enabled assault on violence itself. All past and present political cyberattacks – in contrast to computer crime – are sophisticated versions of three activities that are as old as human conflict itself: sabotage, espionage and subversion … In several ways, cyberattacks are not creating more vectors of violent interaction; rather, they are making previously violent interactions less violent.”

People who understand distributed systems and networks realize this: It may be possible, if hundreds of people work on the problem for years, to damage a single centrifuge facility using a virus – but still only if there’s also a human sabotage agent placed on site. To destroy or disable an entire country’s or region’s infrastructure using lines of code or electromagnetic pulses would be impossible – or, at least, given the need for human agents at each target, it would be the same as using bombs to do so (and bombs would be quicker and easier).

This is Dr. Rid’s crucial message: There is no distinct “online” world; it is simply part of the world, as much as the telephone or the highway. Defence of vital assets remains important, but there is no distinct “cyberspace” to be defended – it is all of a piece.

The danger, Dr. Rid tells me from his office in London, is that the myth of “cyberwar” will lead us to believe that online security is a matter for the military – a notion that the military, eager for funding, is all too willing to promote.

“Hyping a cyberwar doesn’t necessarily create Chinese hackers coming in and harming citizens,” he says. “What’s more realistic is that if we couch the problem in a martial language – war and peace, offence and defence in a military context – then we think that the agencies that are traditionally in charge of that are best placed to deal with the problem, because it’s war. But if you put intelligence agencies in charge of cybersecurity, they’re more likely to apply an offensive mindset to the problem than ministries of interior.”

It is worth spending money to make our computers, and the devices that control our machinery, secure from spying and vandalism. But that’s not war, and it shouldn’t be a job for the warriors.

**Army reserves to become cyber security and intelligence specialists**

Source: http://www.independent.co.uk/news/uk/home-news/army-reserves-to-become-cyber-security-and-intelligence-specialists--and-receive-more-benefits-8684012.html

Reservists in the British Army will become specialists in cyber security, chemical-biological warfare and intelligence under sweeping reforms being carried out to transform the force in preparation for future conflicts, The Independent has learnt.

The Territorial Army, whose size is being doubled from 15,000 to 30,000, will have a much more integrated role to counter the new threats presented by technology and WMDs in the hands of insurgents and rogue states. It will also be extensively engaged in gathering information under plans drawn up by the military.

Philip Hammond, the Defence Secretary, today published a long awaited White Paper on the role of the TA which will be a third of the size of the regular army whose numbers are being reduced by 20,000 to 82,000 in budgetary cutbacks.

The numbers of Royal Navy and RAF reservists will also be increased, albeit on a smaller scale. The numbers of maritime reserves will rise to 3,100 and RAF auxilary to 1,800 from 2,300 and 1,370 respectively.

Reservists will also get military pensions and healthcare benefits under the reforms.

The TA will be to be renamed Army Reserves, and reservists will have enhanced training programmes intended to bring them closer to the standards of the regulars. It is hoped that putting some of them in the cutting-edge field of “intelligent defence” will be an incentive to join and stay in the force.

The Independent has learnt that the Treasury has blocked proposed tax breaks for employers of reservists, available in some states abroad. Instead, employers will receive an enhanced compensation package for staff who are absent on duty. Some reservists could be mobilised once in every five years, taking into account pre-deployment training, and the Government acknowledges that this cannot happen without the goodwill and co-operation of commerce and industry.

The Confederation of British Industry complained last year that it had not been properly consulted on the proposals with director general, John Cridland, saying :“This is the biggest change for reserve soldiers since the Second World War… But we are disappointed by the lack of proper engagement so far.”

Whitehall officials insist that detailed consultation had subsequently followed, although more discussions needed to be held.

The White Paper, it is believed, proposes that employers will have to sign up to a voluntary charter guaranteeing that they will not stand in the way of staff in the TA who have been deployed. They will also pledge to keep their jobs open. At one stage Mr Hammond had  spoken about bringing in anti-discrimination laws such as those defending the rights of women and ethnic minorities to protect reservists, but has now decided against such legislation.

Mr Hammond told the Commons that the changes were "key" to ensuring Britain has the military capability it needs in the coming years.

"The job we are asking our reservists to do is changing," Mr Hammond said.

"The way we organise and train them will also have to change."

There is broad consensus among militaries in the West that cyber security has become a vital part of defence. The head of the Army, General Sir Peter Wall, stressed this when giving the keynote speech at the Land Warfare Conference at the Royal United Services Institute in London last week saying the threats presented by cyber space called for the armed forces to “think and act differently. Control of this domain and with it the ability to defend and attack in order to seize the initiative will be prerequisite for successful operations.”

However, Gen Wall also acknowledged that “The education and personal qualities of our cyber warriors are likely to be a challenge in more linear military behaviour and we therefore need to consider how we recruit and retain experts in the field.”

Military planners point out that these skill-sets already exist among civilians who can bring them to the military while also continuing with their professional careers outside. There are similar pools of knowledge in scientific and linguistic fields which can also be tapped into in relation to WMDs and intelligence-gathering.

The overwhelming likelihood is that combat for UK forces in the foreseeable future will be counter-insurgency operations. Military training teams are being set up for states which are felt to be at risk from instability or coming out of post-conflict situations where knowledge of languages and differing cultures would be of great benefit.

Some former military officers and opposition politicians claim that the Government is being highly optimistic in attempting to raise the numbers of reservists by 100 per cent at a time of recession with deep apprehension about over unemployment.

Among the critics, Colonel Bob Stewart, the Tory MP and Bosnia veteran, had suggested that someone at the MoD was “smoking a lot of dope” to come up with figures which were “pie in the sky”. Labour has accused Mr Hammond of “kowtowing to the Treasury by prioritising austerity over the UK’s national security interests”.

The Defence Secretary insists the projected number is achievable in the timeframe. However, a senior officer said “We would rather go for quality than quantity, that is part of the ethos of this plan. A slight delay in getting the exact number is not a disaster.

“The Army did not decide to lose 20,000 regulars to gain 30,000 reservists on a whim. These are the economic realities, budgetary constraints we face at the moment, like most of our allies. We need to be innovative and make the Army Reserve attractive to high-quality recruits.”

**Volunteer soldiers: Origins of the TA**

The Territorial Force was formed in 1908 by Richard Haldane, the Secretary of State for War, and combined the previously civilian-administered Volunteer Force, militia units and the Yeomanry.

It was the first time the previously separate reserve of part-time and retired soldiers had been regularised.

Shortly before the First World War, the TF was mobilised and soldiers fought alongside regulars in the trenches of northern France, despite the word “territorial” originally signifying that volunteers were under no obligation to serve overseas.

In 1920 its name changed to the Territorial Army, and by 1939 it had doubled in size to 440,000 as the Second World War loomed. After the conflict ended, the TA began to shrink.

With the invasion of Iraq in 2003, it again became increasingly important. Some 6,900 TA soldiers were involved in the hostilities.

They usually have full-time or part-time jobs and attend training sessions in their free time for which **new recruits are paid around £35 a day.**

# Israel army unveils new cyber defense unit

Source: http://www.shanghaidaily.com/article/article\_xinhua.asp?id=152270

The Israeli military offered Monday (July 9th) a peek into one of its most secretive bases, which houses a newly established unit tasked with defending its own networks against mounting attacks launched in cyberspace.

Teams of programmers and computer experts, aged 18 to 22, man the "Cyber War Room," situated at an undisclosed site in central Israel, where malicious cybernetic activities occurring worldwide are monitored around the clock.

Long gone are the days when cyber was the exclusive domain of computer "geeks" spending their nights and days hacking into data bases in the privacy of dimly-lit bedrooms. In the Israeli military, it has already received recognition as another dimension of warfare, alongside the bombers, ships and tank battalions.

"Cyber isn't just another means, but a dimension that exists all the time between and during wars," Brig. Gen. Ayala Hakim, commander of the Israeli Defense Forces's (IDF) Lotam Unit, which oversees cyberdefense operations, told Israel's Channel 10 during an interview Monday.

Israel is investing vast human and financial resources in defending against the immediate threat posed by computer network attacks launched daily on its strategic infrastructure, government ministries, military and intelligence community. The fear is that a major cyberattack could cripple the country's critical infrastructure, including utilities, banking and cellphone networks, among others.

To illustrate the scope of the phenomena, the government revealed it deflected a staggering 44 million attacks on its main online sites during a nine-day war with Islamist group Hamas in Gaza last November.

Last year, the IDF publicly acknowledged for the first time, in a post on its official blog, that it was engaged in both defensive and offensive cyberwarfare. On the defensive end, efforts are mainly focused on repelling attempts by enemy states, global militant networks and lone hackers from overseas to penetrate the military's computers, either for espionage or sabotage.

"The operations room enables us to monitor the great breadth of the Internet at a single focal point," explained the Israeli military official. "We look at what is happening to us via a proactive approach and by gathering open intelligence. We assess our situation."

Like other cyber units operating in Israel's defense institution, including in the intelligence community, the soldiers of the new Cyber War Room constantly seek to increase the nimbleness of their response to identify and prevent an attack, and exploit it to launch a counterattack.

## Federal Standards Body Proposes Cyber Protocols for Private Sector

Source: http://www.nextgov.com/cybersecurity/2013/07/federal-standards-body-proposes-cyber-regulations-private-sector/66005/?oref=nextgov\_today\_nl

The U.S. government has released preliminary guidelines for key industries on how to shield company systems from destructive attacks that could, for example, knock out electricity or halt transportation.

The voluntary rubric, which was released Tuesday afternoon, homes in on the upper echelon of firms. The rationale being that information technology managers can't bolster security without financial and leadership support from top officials, such as board directors.

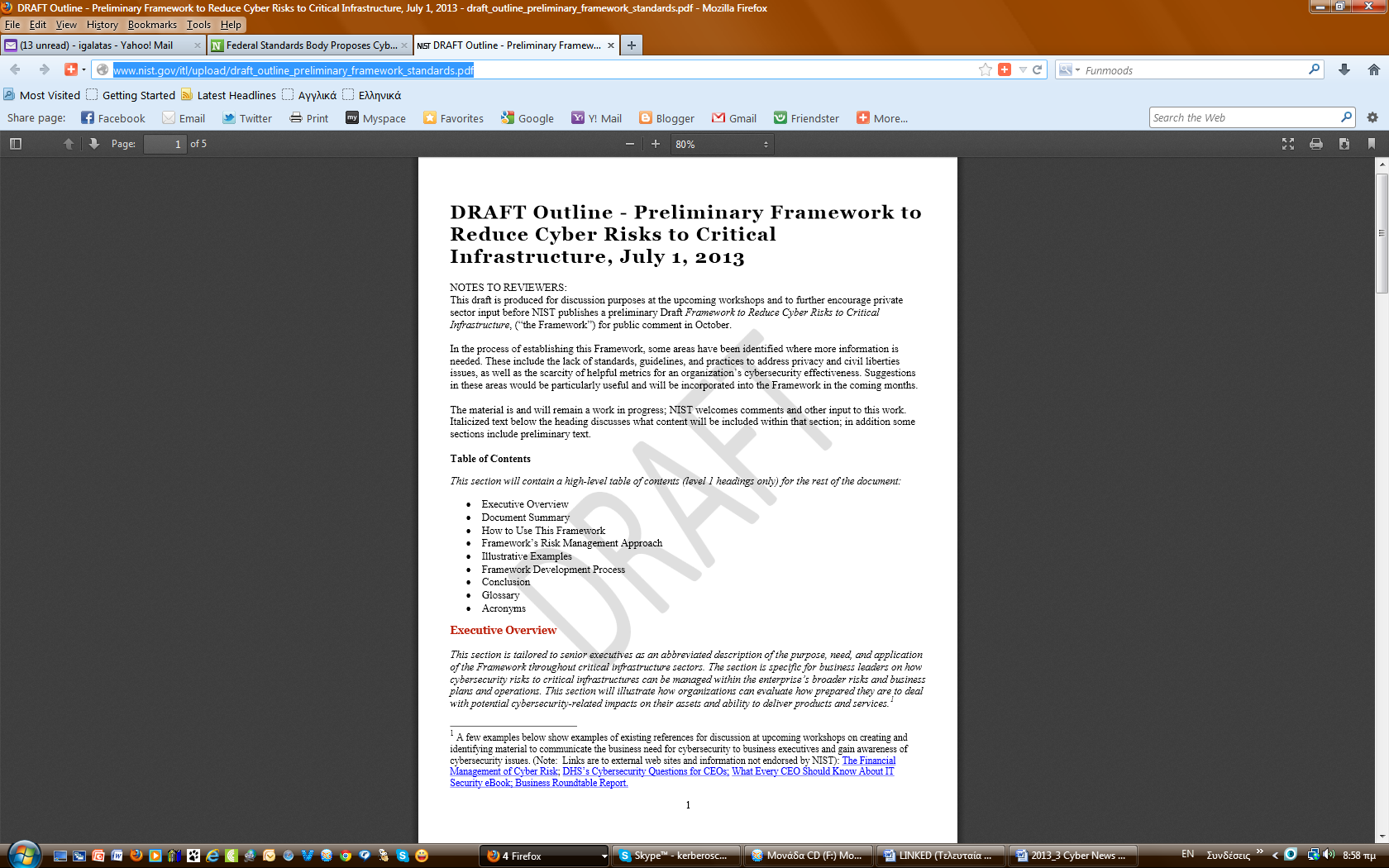
In February, President Obama issued an executive order to protect networks running U.S. critical infrastructure that required the National Institute of Standards and Technology to produce final guidelines by November. NIST officials this week said they anticipate publishing official draft guidelines in October.

Tuesday’s plan includes an information flow chart with five "functions" -- factors that affect companies’ vulnerability levels, including the degree to which firms know, prevent, detect, respond, and recover from threats. Each function includes sub-factors such as contingency planning for the recover category. There also is space to enter relevant industry standards and other existing guidelines, which are provided in a separate document released on Tuesday.

Once a firm fills out the flowchart with applicable information, then there is another chart intended to illustrate the company's current security status.

Each of the five factors is broken down by job position: senior leader, business process manager and operations manager. For the contingency planning subcategory, a senior leader at a company with low-level security might write, for instance, "I'm not sure about redundancy for my critical data," while a firm with a stronger security posture might write, "There is a clear strategic plan in place for the protection of critical data and essential services." An operations manager who works at a firm with low-level security might write, "My organization's critical data is contained in one location."

On Tuesday, NIST officials said the proposed practices reflect feedback from a request for public comment, along with two East Coast workshops and other industry outreach events. Next week, the institute will host a seminar in San Diego. There will be sessions for attendees to complete practice charts, according to NIST officials.

Adam Sedgewick, NIST senior IT policy adviser, said in a statement, "we are pleased that many private-sector organizations have put significant time and resources into the framework development process.”

“We believe that both large and small organizations will be able use the final framework to reduce cyber risks to critical infrastructure by aligning and integrating cybersecurity-related policies and plans, functions and investments into their overall risk management,” he added.

The procedures are optional, and are seen as a stopgap measure until Congress can agree on computer security legislation. Many Democrats would like federal law to mandate that the government enforce such cybersecurity controls, while many Republicans object to regulations and would prefer the government offer companies better threat intelligence. Business leaders have said they need more insights into targeted viruses and more information-sharing among industry about computer breaches.

The order allows such communications, but not liability protections for companies that admit to infected systems.

Some critical infrastructure researchers applauded the administration's attempt to align cyber defenses nationwide.

The plan does "include a lot of moving parts, but information security itself is quite complex.  I think the NIST framework will be helpful for critical infrastructure providers to sort out what their current capabilities are, and what they need to do to have a well-thought-out approach to cyber security.  This is definitely a step forward," said Ed Skoudis, founder of Counter Hack Challenges, which constructed "CyberCity," a 3-D model town that agencies and businesses are using to practice securing  water filtration and other critical industry networks.

►**Read the draft at:** http://www.nist.gov/itl/upload/draft\_outline\_preliminary\_framework\_standards.pdf

# Israel: "Critical entities not prepared for cyber war"

Source: http://www.globes.co.il/serveen/globes/docview.asp?did=1000859417

Scores of water companies, hundreds of food and basic goods factories, pharmaceuticals manufacturers and distributors, and important financial institutions must take major steps to protect their computer systems against cyber attacks, Institute for National Security Studies (INSS) cyber warfare program director Dr. Gabi Siboni told "Globes".

Siboni's remarks are based on comprehensive staff work which he is heading on the subject. The study's main points will be submitted as recommendations to the relevant government ministries and to the Israel National Cyber Bureau at the Prime Minister's Office, which is drawing up an optimal defense concept against cyber threats in the civilian arena.

"Cyber defense in the civilian arena is not being dealt with, in contrast to the defense sector, including defense industries, and scores of critical national infrastructures, because they receive regular guidelines on the issue from government departments," says Siboni. "But telecommunications carriers, including Internet service providers and other entities with systems which, if attacked, are liable to substantially disrupt service to a large clientele, are not defined by the government as critical infrastructures, and there is no authority which directs them how to prepare against a possible cyber attack. While dozens of critical national infrastructures are protected, someone deciding on an attack will prefer to focus his efforts on the soft underbelly, against those who are unprotected. The target could be the water company of a large city. Today, water companies and critical entities in the economy are not prepared for such a situation, because no one demands that they should prepare."

**Start with the financial world**

Siboni will present the main points of his plan at an INSS conference next week on the financial industry's preparedness for a cyber attack. He says, however, that his position is not representative of all his colleagues on the forum which is discussing the issue. He proposes that the solution to the gap between the ever increasing threat of cyber attacks and the scale of preparedness by the civilian arena against them should lie with the regulators of the different entities, who will receive guidelines from an umbrella organization responsible for cyber defense in the civilian arena.

"When a business of any kind goes to the authorities to obtain a license for its activity, it has to meet many requirements in the areas of environmental quality, the handling of hazardous wastes, sanitation, the electricity system, approval from the fire department, etc. No one dictates to the relevant business-owner threshold conditions for cyber defense," says Siboni.

Siboni says that civilian enterprises and organizatons should be ranked according to their how critical they are to the economy in an emergency, and that on this basis they should be assigned to one of 4-5 categories. For each category, there will be threshold conditions which these entities will be required to meet for protecting information systems and various operating systems, and they will submit a detailed review which will examine the survivability of the organization's systems in the face of a cyber attack.

"We should avoid a situation of establishing another regulator in the country. It will be possible to implement these regulations through the existing system: the Water Authority, which is the regulator of the municipal water companies, will also supervise their cyber preparedness; and the same will apply to other sectors. The regulator will be given the authority, the criteria, and regular updates on network attacks from the central organization that will be set up, and this will be binding regulation on the entities in its sector," says Siboni.

As for the huge damage and disruption to day-to-day life from a targeted cyber attack, the Siboni-led forum believes that fairly simple and inexpensive measures can foil them. "All in all, it is necessary to invest thought in the authorization of access to the computer systems of every organization, to ensure that there are command and control systems, and to isolate systems that are critical for day-to-day operations from other systems, establishing separate defense systems. This is not too expensive, but definitely requires alertness," he says.

"I identify the financial world as the best place to begin providing a good response to the emerging cyber threat. Everywhere in the world, cyber attacks are used for online fraud, and crime in this area is huge. Since the common denominator of all financial institutions in the world is money, they represent an excellent platform for developing for developing an appropriate response to the cyber threat in the civilian arena."

## Napolitano leaving DHS post

Source: http://www.homelandsecuritynewswire.com/bull20130712-napolitano-leaving-dhs-post

**DHS secretary Janet Napolitano announced that she would be leaving her post in early September to become president of the University of California system.**

Her resignation is surprising, because the former governor of Arizona was seen as a potential successor to under-pressure Attorney General Eric Holder, if he were to leave his post.

In a statement released Friday morning, Napolitano said: “The opportunity to work with the dedicated men and women of the Department of Homeland Security, who serve on the front lines of our nation’s efforts to protect our communities and families from harm, has been the highlight of my professional career.” The The Washington Post reports that Napolitano served as DHS chief during a contentious and event-filled period which saw her department dealing with issues such as immigration, border security, the Boston bombing, Superstorm Sandy, and deadly tornadoes in the Midwest.

In her statement, Napolitano added, “The Department has improved the safety of travelers; implemented smart steps that make our immigration system more fair and focused while deploying record resources to protect our nation’s borders; worked with states to build resiliency and make our nation’s emergency and disaster response capabilities more robust; and partnered with the private sector to improve our cybersecurity.”

President Obama thanked Napolitano for her more than four years of service, saying, “Janet’s portfolio has included some of the toughest challenges facing our country.”

“The American people are safer and more secure thanks to Janet’s leadership in protecting our homeland against terrorist attacks,” Obama said in a statement. “I’ve come to rely on Janet’s judgment and advice, but I’ve also come to value her friendship. And as she begins a new chapter in a remarkable career of public service, I wish her the best of luck.”

The sprawling University of California system, the largest in the nation, has ten campuses with 220,000 enrolled students, more than 170,000 faculty and staff, and an annual budget of $24 billion.

The New York Times notes that Napolitano does not have an extensive background in education, but the California university system saw her extensive management experience running a state and one of the largest federal government bureaucracies as assets.

“While some may consider her to be an unconventional choice, Secretary Napolitano is without doubt the right person at the right time to lead this incredible university,” the former film studio executive Sherry Lansing, who headed the search committee, said in a statement to the Los Angeles Times.

The Post notes that the two leading candidates to replace Napolitano are two insiders who, unlike Napolitano, have good relationship with congressional oversight committees.

FEMA administrator W. Craig Fugate, who had worked for two Republican governors in Florida, where he served as the director of the state’s emergency management.

TSA head John Pistole, has built good relations with Congress despite objections over recent proposed changes to screening procedures at airports.

## Napolitano warns of a “cyber 9/11”

Source: http://www.homelandsecuritynewswire.com/napolitano-warns-cyber-911

DHS secretary Janet Nepolitano last week  said that a coordinated cyber attack on the United States – in effect,  a cyber 9/11 — could happen.

“We shouldn’t wait until there is a 9/11 in the cyber world,” Napolitano told Reuters. “There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage.”

TopTechNews quotes Chris Peterson, the chief technology officer of LogRhythm, to say  that it is unfortunate that the president has to use an executive order to protect critical infrastructure.

“Ideally, Congress would recognize and act on the threat we face as a nation when it comes to defending ourselves against cyber war and cyber terrorism. These threats are real and will only increase in the years to come — drastically and swiftly,” Petersen told TopTechNews. “If signing an executive order does nothing other than help move cyber security spending up the stack of 2013 IT budgets, it will be a win for us all.”

According to Petersen, there are  valid concerns when it comes to cyber legislation,for example,  the additional compliance burdens on U.S. companies. Petersen said, though, that without a baseline companies will not know whether their systems are protected, and without enforcement, some companies will just think they can take protective measures sometime in the future instead of now, and hope for the best.

“We appreciate that there are valid concerns and criticisms that will be disclosed through discussion. However, there is real risk in delaying action as we wait years for all opinions and concerns to be aired,” Petersen said. “We need immediate action with continued refinement in years to come. For example, this refinement could be an industry taking a self-regulating approach similar to NERC-CIP in the energy sector or PCI in retail.”

Amrit Williams, CTO of Lancope, says the threat of a massive attack on critical infrastructure, both public and private, should be enough for the Obama administration to do whatever is necessary to regain control and thwart the threat, but he also admitted that is easier said than done.

“This is a massive logistical problem, growing even more so as technology advances and becomes adopted as part of our digital fabric. Unfortunately there will be mistakes, errors in judgment, and poorly written policies that may very well lead to significant self-inflicted damage,” Williams told TopTechNews.

# Emergency broadcasts 'can be hacked'

Source:http://www.terrorismwatch.org/2013/07/emergency-broadcasts-be-hacked.html?utm\_source= feedburner&utm\_medium=email&utm\_campaign=Feed%3A+terrorismwatch%2FJTvK+%28Terrorism+Watch%29&utm\_content=Yahoo!+Mail

The system used to broadcast to the United States in times of national crisis can be hacked, researchers have warned.

The Emergency Alerting System (EAS) was set up to allow the president to talk to the entire country within 10 minutes of a disaster.

Security specialists IOActive said one TV network's output "was interrupted by news of a zombie apocalypse".

Lead researcher Mike Davis said the system needed to be re-engineered.

IOActive has released a guidance sheet for concerned broadcasters looking to protect their system.

**'Extremely dangerous'**

In February, weaknesses in the system - which was introduced in 1997, replacing an older set-up - were exposed by hackers.

"Earlier this year we were shown an example of an intrusion on the EAS when the Montana Television Network's regular programming was interrupted by news of a zombie apocalypse," said Mr Davis.

"Although there was no zombie apocalypse, it did highlight just how vulnerable the system is."

The message, which was also played out on a radio station in Michigan, said: "Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living.

"Follow the messages onscreen that will be updated as information becomes available.

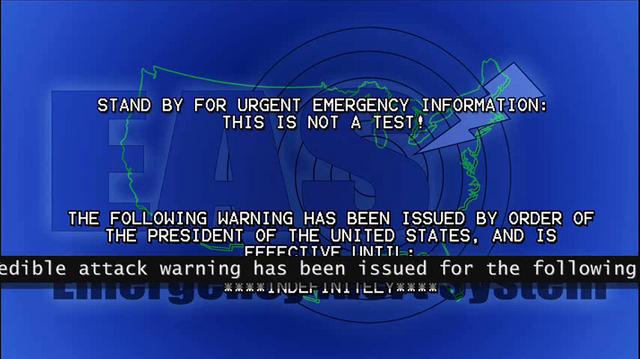
"Do not attempt to approach or apprehend these bodies as they are considered extremely dangerous."

Station bosses later apologised for any alarm or distress to listeners brought on by the unexpected alert.

**UK testing**

In the UK, no such emergency broadcast system is in place.

"We don't have an alerting system similar to that in this country at the moment," a Cabinet Office spokeswoman told the BBC.

However, the government is set to launch trials later in the year of a new "public emergency alert system".

Mooted plans include alert systems which span a variety of platforms, including the internet and mobile.

Social media will also be key, according to consultation documents published on Gov.uk.

"The popularity of social media makes it an ideal platform for communication with people and for disseminating additional information in the aftermath of an emergency," the document reads, before remarking that security must be a high priority to prevent false alarms.

If a national emergency were to take place today, broadcasters such as the BBC have contingency plans to ensure broadcasts can continue even if key locations are inactive.

# The typewriters are back in the Kremlin

**Source: http://i-hls.com/2013/07/the-typewriters-are-back-in-the-kremlin/?utm\_source=activetrail&utm\_ medium=email&utm\_campaign=English%20Newsletter%2010/7/2013**

****

**A source at Russia’s Federal Guard Service (FSO), which is in charge of safeguarding Kremlin communications and protecting President Vladimir Putin, claimed that the return to typewriters has been prompted by the publication of secret documents by WikiLeaks, the whistle-blowing website, as well as by Edward Snowden, the fugitive US intelligence contractor.**

 According to the Telegraph the FSO is looking to spend 486,000 roubles – around £10,000 – on a number of electric typewriters, according to the site of the state procurement agency,  zakupki.gov.ru. The notice included ribbons for German-made Triumph Adlew TWEN 180 typewriters, although it was not clear if the typewriters themselves were of this type.

The service declined to comment on the notice, which was posted last week.

However an FSO source told Izvestiya newspaper: “After scandals with the distribution of secret documents by WikiLeaks, the information exposured by Edward Snowden, reports that Dmitry Medvedev was being listened in on during his visit at the G20 summit in London, it has been decided by us to expand the practice of creating paper documents.”

Unlike printers, every typewriter has its own individual pattern of type so it is possible to link every document to a machine used to type it.

 “Typewriters are still used to type on paper with an adhesive layer so that the glue doesn’t get too hot,” the source said. “What’s more, a whole series of documents are not created on electronic devices. That practice exists in the defense ministry, the emergencies ministry and the special services.”

Directives to the defense minister and the supreme commander-in-chief, Mr. Putin, are still printed on paper, a defense ministry source said.

Documents leaked by Mr. Snowden appeared to show that Britain spied on foreign delegates including Dmitry Medvedev, then the president, at the 2009 London G20 meetings.

Russia was outraged by the revelations but said that it had the means to protect itself.

Mr. Snowden has been stuck in the transit zone of Sheremetyevo Airport in Moscow for three weeks since arriving from Hong Kong in a bid to seek asylum.

Nikolai Kovalev, the former director of Russia’s Federal Security Service, told Izvestiya: “From the point of view of security, any means of electronic communication is vulnerable. You can’t remove any information from a computer. There are means of defense, of course, but there’s no 100 per cent guarantees they will work. So from the point of view of preserving secrets the most primitive methods are preferable: a person’s hand and a pen, or a typewriter.”

However, another expert said that paper documents were still unreliable because they could be stolen, photographed, or could go up in smoke in case of a fire.

# “Cyber Attack on the U.S. Could be Met with Conventional Military Response”

Source: http://i-hls.com/2013/07/cyber-attack-on-the-u-s-could-be-met-with-conventional-military-response/?utm\_source=activetrail&utm\_medium=email&utm\_campaign=English %20Newsletter%2010/ 7/2013

CYBER attacks on U.S. infrastructure or networks could be met with a conventional military response, the chairman of the Joint Chiefs of Staff Army Gen. Martin E. Dempsey warned. “The rise of CYBER is the most striking development in the post-9/11 national security landscape,” Dempsey told the audience. “We are doing everything we can inside the military to be ready to operate in CYBER space.

“There is an assumption out there … that a CYBER attack that had destructive effects would be met by a CYBER response that had destructive effects,” Army Gen. Dempsey said to an audience at a Brookings Institution forum. “That’s not necessarily the case. I think that what [President Barack Obama] would insist upon, actually, is that he had the options and the freedom of movement to decide what kind of response we would employ.”

The impact of a CYBER attack is a key question for elected officials to answer when considering the level of response, Dempsey said. “When does CYBER theft become a hostile act?” the chairman asked. “Or when does CYBER theft, added to distributed denial of services, become a hostile act? Or is a hostile act simply defined as something that literally is destructive in nature?”

CYBER has many features in common with other domains, and shouldn’t be thought of as a wholly exceptional realm, Dempsey continued. Although it can sometimes feel abstract, he explained, CYBER is a physical domain in the sense that it is operated by men and women over routers and servers, and CYBER attacks can result in real, physical damage.

“I think that to the extent that we can always think about it in the way that we’ve always organized our thinking about the other domains, it might illuminate the challenge a little better,” the chairman said. “I do think that there are capabilities out there that are so destructive in nature and potential that it would be very difficult not to see them as acts of war.”

But, he noted, “the decision to declare something a hostile act — an act of war — is certainly one that resides in the responsibility of our elected leaders.In its mission to defend the nation, the Defense Department must stay ahead of the ongoing technological revolution and its attendant rise in “anywhere, any time” CYBER threats, the chairman of the Joint Chiefs of Staff said here today.

“One thing is clear: CYBER has escalated from an issue of moderate concern to one of the most serious threats to our national security,” Dempsey said. Now, the entire country could be disrupted by the click of mouse, he added. To address these threats, the military must take on new missions, the chairman said.

“CYBER incidents have steadily escalated over the past year, Banks and oil companies have been targeted by sophisticated attacks, he said, and more than 20 nations now have military CYBER units… This is the new normal in cyberspace,” Dempsey said. “Disruptive and destructive cyberattacks are becoming a part of conflict between states, within states, and among nonstate actors. The borderless nature of cyberspace means anyone, anywhere in the world, can use cyber to affect someone else.”

It isn’t enough to just strengthen cyber defenses on military systems, the chairman said. Intrusion attempts on critical civilian infrastructure systems have increased 17-fold over the last two years, he said. “The gap between cyber defenses deployed across critical infrastructure and offensive tools we now know exist presents a significant vulnerability for our nation,” Dempsey said.

In response to the threat, the Defense Department is growing its capacity to protect its own networks, and it’s adding a new mission: defending the nation, when asked, from attacks of significant consequence — those that threaten life, limb, and the country’s core critical infrastructure, the chairman said, announcing that over the next four years, 4,000 cyber operators will join the ranks of U.S. Cyber Command, and $23 billion will be invested in cybersecurity.

Three types of teams will operate around the clock at Cyber Command, Dempsey said. National mission teams will counter adversary cyberattacks on the United States. A second and larger set of teams will support combatant commanders as they execute military missions around the globe. The largest set of teams will operate and defend the networks that support our military operations worldwide.

Although the Defense Department has made significant progress in embracing cyber, the nation’s effort to protect critical civilian infrastructure is lagging — a worrisome vulnerability, the chairman said.Sharing information about cyber threats is one of the most important ways to strengthen cybersecurity across the private sector, he added, but threat information primarily is shared in only one direction: from the government to critical infrastructure operators. “That has to change,” Dempsey said. “We can’t stop an attack unless we can see it.”

The most immediate priority is securing the “dot-mil” domain, the chairman said. “But in the event of a domestic cyber CRISIS,” he added, “our cyber forces will work in support of the Department of Homeland Security and the FBI, who lead our nation’s response in the dot-gov and dot-com domains.”

To ensure this force is able to operate quickly, the Defense Department now has a “playbook” for cyber, Dempsey said, noting that a presidential directive codifies how each part of the government will respond in the event of a serious cyberattack. Under this directive, the department has developed emergency procedures to guide its response to imminent, significant cyber threats, the chairman said. The Defense Department is updating its cyber rules of engagement for the first time in seven years, he added, and also is improving mission command for cyber forces.

While cyber may be the nation’s greatest vulnerability, Dempsey said, it also presents the military with a tremendous asymmetric advantage. “The military that maintains the most agile and resilient networks will be the most effective in future war,” he told the audience. “This is the kind of force we are building for the future.”

Each branch of the military is doing its part, the chairman said, by investing in equipment and personnel that will ensure the joint force can operate in cyberspace as capably as it can on land, sea, air, and space. The next step is the planned Joint Information Environment, he said — a single, easy to secure, joint network delivering data to the department’s personnel wherever and whenever they need it.

“As part of this new Joint Information Environment, we’re building a secure 4G wireless network that will get iPads, iPhones and Android devices online in 2014,” the chairman said. “With tools like this, the smartphone generation joining our military will help us pioneer a new era of mobile command and control.”

# Cyber Jihad: Jihadist Use of the Internet 2008-2011

Source: http://privacy-pc.com/articles/cyber-jihad-jihadist-use-of-the-internet-2008-2011.html

**Jeff Bardin** from Treadstone 71 provides a detailed overview of the Jihadist activities on the Internet, including their software tools, online resources, etc.

Good day and welcome to this cyber jihadist use of the Internet from 2008 to 2011 overview by Treadstone 71. This deck, over 60 slides, will cover from a high level the jihadist use of the Internet through those years, actually starting well before 2008, but first delivered by myself in different seminars, discussions, talks from RSA and SecureWorld Expo.

**Diversified language support**

These discussions are compiled here into one deck. I removed some information I thought was not important for this talk, but hopefully it will provide you some education on the level and types of use of Islamic extremists and their use of the Internet over those years.

This slide (photo) demonstrates their use of audio and video in multiple different languages. They’ll use German, Spanish, Turkish, English, as well as Arabic. You will also see videos out there that are meant to shock; others are meant to educate and teach and train, others are meant to brainwash and continue the standard view of the Salafi view of Islam.

**Collage on Jihadist resources**

This particular slide (on the left) is a series of animated gifs that focus on some more training, like the Mujahideen Poisons Handbook, which is a little bit like an instruction; the Mujahideen Secrets v.2, the encryption tool (there was version 1, we’ll cover that a bit later), as well as some other animated gifs here on 9/11 and ambushes throughout the Iraq war era.

**Agenda**

The agenda for today is: we’re going to cover online training and look at jihadist media out there. We’ll look at the Salafi with respect to radicalization; also take a look at forensics and communicating jihad. And then we’ll close up for the day and wrap it up. This is over 60 slides, so it is lengthy, even though this subject could go on for days and weeks, if we had the time. Hopefully you’ll enjoy the presentation.

**Jihadist online training resources**

There was a great deal of training early on (photo below). There was Al-Battar magazine, and they had several issues focusing on training, a training camp. The 6th issue, which you can see the cover here on the right, discussed cell organization and different command structures for their cells.

They also had a magazine that came out with two editions called The Technical Mujahid. These were all in Arabic and talked about more IT technical type of issues, as well as some violent type activities.

Then there was the Al-Qaeda University for Jihad Sciences that was electronic. It talked about e-Jihad, and we’ll talk about some of that a little bit later. There are training manuals out there and videos for explosives of all types, IED’s, surface-to-air missiles, flying planes – there were just 18 videos on flying 747’s back in the Al-Battar video days.

There was one issue here, issue #10 of Al-Battar that was a training manual focusing on special coverage of kidnapping. It had reasons for detaining one or more individuals by an enemy and forcing the government or the enemy to succumb to some demands, put the government in difficult situation that will create a political embarrassment between the government and the countries of the detainees; obtaining important information from the detainees, obtaining ransoms, which we’ve seen a lot of late. Such was the case with those in the Philippines, Chechnya and Algeria in the early days. They say that brothers from Mohammed’s army in Cashmere received a 2 million dollar ransom that provided good financial support to the organization, able to fund other terrorist activities.

I’ll bring a specific case to light; this happened at the beginning of the cases in Chechnya and Algeria with the hijacking of a French plane, if you remember that. And the kidnapping operations were performed by the brothers in Chechnya and the Philippines.

There were just 18 videos on flying 747’s back in the Al-Battar video days.

They also have requirements needed in forming a kidnapping group: a capability to endure psychological pressure in difficult circumstances. In case of public kidnapping the team will be under a lot of pressure, they say. And the detention must not be prolonged: “in case of stalling, hostages must be gradually executed so that the enemy knows we are serious.”

“When releasing hostages such as women and children, be careful as they may transfer information that might be helpful to the enemy. You must verify that the food transported to the hostages and kidnappers is safe – this is done by making the delivery person and the hostages taste the food before you. It is preferred that an elderly person or child brings in the food, as food delivery could be done by a covert Special Forces person.”

“Beware of the negotiator: stalling by the enemy indicates your intention to storm the location. Beware of sudden attacks, as they may be trying to create a diversion, which could allow them to cease control the situation. Combat teams will use two attacks, the secondary one just to attract attention, and the main attack elsewhere. In case your demands have been met, releasing the hostages should be made only in a place that is safe to the hostage takers. Watch out for the ventilation, or rather openings, as they could be used to plant surveillance devices, through which the number of kidnappers could be counted and gases could be used.”

“Do not be emotionally affected by the distress of your captives. Abide by Muslim laws as your actions may become a dower call to join Islam. Avoid looking at women.” These are just some of the training items in issue #10 of Al-Battar.



**Lessons from training manuals**

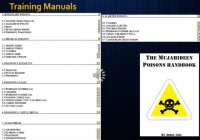
Other training manuals (photo) covered many different lessons out there – from counterfeit currency and forged documents to weapons, measures related to buying and transporting them, special tactical operations, espionage, information gathering using open methods, open source in this case, or covert methods, and the secret writing with ciphers and codes, as well as assassination using poisons and cold steel. We’ll take a look at some of that with respect to cold steel in the next slide.

**Assassination training**

With respect to assassinations (see left-hand image) using cold steel they get very descriptive on where to actually place the blade: anywhere on the ribcage, both or one eye, the pelvis, the back of the head, the end of the spinal cord – directly above the person’s buttocks; made to disable and kill as much as possible, as quickly as possible.

In addition, they talk about the blow of a club between the eyes, veins and arteries, genitals and so on. They get into specifics of grabbing testicles, grabbing the ribcage, and how to actually perform the execution in a battle, in a fight. They also talk about castor beans and ricin in detail in multiple different documents out there and training manuals. This is just one, and it gets very specific in how to go about performing these actions. So what you have online is a basis for academic side of training, and then you have to go to a training facility in different territories where they have these camps, and actually learn how to do it firsthand.

**The Mujahideen Poisons Handbook**

I mentioned in one of the slides earlier the Mujahideen Poisons Handbook. This is the index (photo), one of the indices in the beginning here, actually, a table of contents. And it talks about homemade poisons from ricin, alkaloids of potato, arsenic, sodium nitrate, thallium, and phosphorus to chlorine and different gases. The edition starts with introduction: this file is dedicated to help folks learn how to put together different poisons.

“May Allah reward him every time it is used in his path and may He help him in his difficulties, amen. To the mujahideen of Afghanistan who’ve lit the flame of jihad in the hearts of every sincere Muslim. Throughout the world you will conquer Constantinople and Rome.” This is from the Prophet Muhammad, peace be upon him.

**Details on a specific poison**

They go on to talk about the book dealing with poisons (photo), and poisons are substances which cause harm to human body, of course. It is an esoteric knowledge, and must only be passed on to those who truly intend to use it in the name of Allah. They talk about lethal doses that often have a question mark beside them – that is because the quantities given are not established truly; they’re only estimates based on experiments with rabbits.

It is hoped that the brothers who work on this subject will research further, care out their own experiments, and refer to medical books to fill in what is missing. So they do realize that there’re holes here and it’s actually just a starting point. The gentleman who publishes this goes on to say: “I was learning from people whose first language was not English; some of the names of chemicals, properties are wrong. Be very careful when preparing poisons: it is much more dangerous than preparing explosives. I know several mujahids whose bodies are finished due to poor protection. On the positive side, you can be confident that poisons have actually been tried and tested successfully, hehe.” So this is the mujahideen poisons; that’s been out for several years and it’s still available out there. And again, I’ll focus here on ricins, since it’s been in the news frequently lately in the United States.



**Jihad Recollections magazine**

Now, most people believe that Inspire magazine was the first jihadist magazine, but actually Jihad Recollections was (photo). Here in this edition we have “Obamaturk”, comparing Obama to Ataturk, the then leader of Turkey, the Ottoman Empire, who brought secular vews to Islam, which is directly an anathema to the Islamic extremists view, the Salafi view of Islam.

**Discussions on Adam Gadahn**

In addition we have some discussions here on Omar Hammami and his conversion to Islam and move to fight with the Shabab in Somalia. In addition we have Adam Gadahn, who had gone from Jewish to Christian values to Islam to extremist Islam coming out of Los Angeles, who is now married and reported to be living in Pakistan as one of the spokesmen (photo). Adam has been very adamant; many see him as quite a buffoon, but he still continues to communicate in English, as well as in Arabic, Salafi values. So the intent here is to demonstrate that many westerners have seen the light and have converted to Islam.

In addition, in this particular version as of May of 2009, we have a warrior trainer, the days of Abu Leith; we have the analysis of the architect of global jihad, which is from Abu Musab al-Suri who was released from jail in Syria during the recent activities over there.

Revisiting the global jihad media effort is discussed in this, talking about America being a bully among bullies, and different activities about technology with respect to: “Forget cell phones, the sixth sense is coming,” and 8 great reviews of iPhone 3.0. So they cover many different things in this from religion and biography, strategy and lessons, social issues, technology, and health, and the jihad recollections. There were four versions that made it before this magazine actually was retired.

**More on Jihad Recollections**

Continuing onto this version of Jihad Recollections from May 2009: you see information here on the left from GIMF, the Global Islamic Media Front (photo), on a video: “Signs of Victory are Looming over Afghanistan.” At the bottom on the left you see a pointer that points to one of the online storage sites, at the time – FileFlyer. On the right you see more discussion on the war of atrocities from the same gentlemen, and a pointer down the bottom to FileFlyer again.

But the text here is from Abu Musab al-Suri, criticizing some of the issues with respect to current training and activities and success rates of the different schools out there, and really hitting home at this failure in education due to the lack of a program, and there’s a political failure, because there is absolutely no program.

In the Salafi view of Islam they offer no programs, no training from political viewpoint and no establishments from a political organization. So once they take over, it’s just pure chaos for the most part. They say that they’ll refer back to the Islamic law, but their interpretations are extremely severe, and people suffer at the hands of it.

You will also find that al-Suri is looking for more mobile training methods, such as in-house training. He also goes on to talk about online training and just-in-time type training using means that secret and subtle and creative while using effective methods to strike as much pain, loss and terror to the adversaries.

**Technical Mujahid**

This is a screenshot from Teqany magazine (photo); it was in Arabic exclusively. It was a technical magazine focusing on teaching and training on how to use various tool sets available in the marketplace. First released in November 2006, there were only two editions of this particular magazine.



**Training set on Teqanymag**

From the inside of Teqanymag you have methods on how to hide documents. On the top left you also had GPS utilization focusing on Iraq at the time. Use of wireless devices and video and media players out there was also part of their standard training set with respect to Teqanymag (photo).

**Growth of e-Jihad**

Back in 2007 there was an effort to take down different sites that were criticizing the Muslim sites, or, in particular, the Salafi-type sites. Raising e-Jihad was this effort (photo below); as you can read from the right here, they’re trying to get people to sign up. One of the unique things about this was the video game atmosphere around what they were trying to do.

It says that the program provides a number of hours for an attack, in this case 24. They are going to update their databases. They have features, such as direct communication with the leadership and business networks, especially from the heavens. And their names will appear on this page per period, each period between a month and two weeks after this is done with the authorization of Allah.

They had an option to register a username in writing of who’s been invited to participate, and it led up to 24 points, one per hour for each brother brought in to join the attack. The strategy here is to find locations out there, to have them withdraw data that is actually abusing Muslims or is against their values. And the attack that they wanted to hit them with is doubling or tripling their bandwidth usage for denial-of-service. And they would really prefer to push them into bankruptcy and close the site if possible.

They indicate that the attack will be open for 24 hours and that members can collect the greatest number of points, with each point being equivalent to one hour of attack. This never really matriculated, but the effort started early on, and that is what we see on the next slide. There was a tool put out there in several versions of a DDoS-type tool.

**Electronic Jihad program’s features**

They followed on with a new Electronic Jihad program (photo below) starting with version 1 to 1.5, eventually 2 and moving on to version 3. They made this much more simple to use. They made software downloads to simplify the denial-of-service attacks. It was designed by a Saudi national. They had chat rooms available to plan and coordinate attacks. And there was a forum that listed websites to be attacked and the potential impact they wanted to carry out.

So, unlike the first campaign of electronic Jihad where participants did not have prior knowledge of the websites that they were attacking until they activated the Electronic Jihad software, the main page of the then al-jinan.org site carried names of the websites to be targeted for the attacks. Also the e-Jihad software program 1.5, or the silver version, had been updated to v.2 and again to 3. The new version of the software was much easier to use. After a few seconds of activation it actually updates the targets automatically and is compatible with different connection speeds and capable of using different proxies to override different website blocking technologies.

The version also set up account name and passwords at al-jinan.org for every user. And they can register the number of hours the user spent attacking targets and every two weeks the names of those who scored the highest would actually be posted. At the time the highest score was claimed by user nicknamed George Bush, who spent 4211.5 hours, or 70 full days, trying to DoS anti-Islamic sites. Other users spent hundreds of hours running the program as well.



**Electronic Jihad version 3.0**

The installation process for the Electronic Jihad program is very simple, you just need to follow instructions and click through. In addition it shows you the interface for Electronic Jihad (photo), much the same as before, but this is a 3.0 version with more features.

**Secure download for Electronic Jihad program**

In addition, what they followed on with is where you at the time could download e-Jihad 3.0.zip, guaranteed by Kaspersky to be clean of any malware (right photo). So, very simple to find at the time; probably, nowadays you’d find it at archive.org, the way back machine which continues to archive pretty much anything and everything of Jihadist value and makes it available for them.

**Tool for conducting DDoS attacks**

There was another tool made available at the time that was much the same with respect to DDoS, or denial-of-service type of attacks (photo). What they were really after here was conducting these different cyber attacks or hacking for money and organizational support, disruptive hacking for cyber Jihadist against different websites out there. And what they’re looking for is trying to acquire different low-level weapons for development and training here and distributing these hacking tools and information about them and educating people on how to use them, and then having statements as well about computer network attacking activities.

They would look for calls for action here, and formal education in IT. And they looked at cyber space experience as something that they were after here, and the extensive use of the Internet was what they sought. And again, the development use of cyber tools, including network and data security tools, were key areas that they were recruiting for in the online forums.

**To be continued…**

# Holistic Security - Various Ways to Reduce Vulnerability

**By Armond Caglar**

Source:http://www.domesticpreparedness.com/Infrastructure/Cyber\_&\_IT/Holistic\_Security\_-\_Various\_Ways\_to\_Reduce\_Vulnerability/

According to a May 2013 report of the Commission on the Theft of American Intellectual Property – an independent, bipartisan initiative of U.S. representatives from both the private and public sectors – the theft of intellectual assets is estimated to cost U.S. businesses more than $300 billion annually. Increasingly, U.S. companies are not only facing persistent threats to the integrity of their business activities, but also grappling with the need to stem the erosion of their companies’ values caused by commercial espionage carried out by both foreign and domestic actors.

In addition to the harm caused to the businesses directly affected, such thefts also contribute to a significant loss of U.S. jobs and a corresponding decline of the national economy in terms of a reduced gross domestic product. In some cases, the thefts also have resulted in the loss of U.S. ingenuity to rivals who are not only stealing intellectual property but also counterfeiting and/or otherwise adapting that property to foreign markets by focusing on low-cost positioning and mass consumption – both of which subsequently evolve into market disruptions in their own right.

These challenges have been not only costly but also fairly consistent in recent years. According to the 2012 Cost of Cyber Crime Study of 56 U.S.-based companies (many of them multinational corporations) – sponsored by Hewlett-Packard and carried out by the independent research group Ponemon Institute – cyber espionage attacks have increased by an average of 38 percent from 2010 to 2011. The average annual cost for the companies included in the 2012 study amounted to approximately $8.9 million. Moreover, the World Intellectual Property Organization headquartered in Geneva, Switzerland, estimated that, “In 1998, intangible assets constituted 80% of the value of Fortune 500 companies.” Obviously, the potential for truly extraordinary losses in the foreseeable future is not only evident but also probable.

**Protecting U.S. Companies From Cyber Threats**

Although investments in protective measures such as firewalls and/or anti-virus solutions are popular options, they are insufficient in isolation. In an age of sophisticated and frequent attacks, particularly as related to the state-sponsorship of intellectual property theft through cyber and insider threats, private firms – the U.S. government as well – must ensure that security investments are diversified throughout their entire business plans and operations.

Diversification does not necessarily mean, though, that security investments in specific components of an enterprise do not provide protection. They certainly can, and often do. The problem is that securing individual components does not secure the business as a whole. Some software vendors may purport to sell their products as the one and only “cure-all” needed for total security and protection. But new technology added to a company’s existing security infrastructure creates additional complexity. One likely result is that at least some of the company’s data may not be properly analyzed and correlated with other data that the same firm creates.

Application behavior, system performance, user actions, and deceptive activity are all critical data streams that can serve as invaluable intelligence in any post-incident investigation – or, preferably, pre-incident assessment. However, if such information is not used properly, and in conjunction with other data, an organization may find significant losses related to its product designs, research and development (R&D) operations, competitive processes, patents, and other intellectual property.

For other enterprise-specific issues such as information technology (IT), the outsourcing to IT risk consultants can offer well-known approaches for understanding a firm’s ability to fend off attacks. However, the expertise of those consultants often focuses primarily on risks within the IT structure – despite the fact that there are many other potential areas of risk that must be taken into account to fully protect a company’s intellectual property.

For companies that rely on in-house personnel to meet their security needs, the basic problem remains the same. Although some organizations often prefer this solution – usually for fear of not wanting to reveal vulnerabilities to outsiders – company personnel frequently focus their attention primarily on diagnostics, forensics, and basic security monitoring. Often, because of the nature of their employment, staff members: (a) may not be able to offer an objective assessment; and/or (b) do not necessarily possess a high enough level of expertise, and the investigative skills also required, to carry out a truly comprehensive analysis of the company as a whole.

Rather than focusing on security solutions in only one component of a firm’s operations, a holistic intelligence program would diversify the collection of information across the entire enterprise. Use of this broader approach usually will help protect the intellectual assets of public- and private-sector organizations in the current age of sophisticated threats.

**Holistic Security: A Deeper Look**

Holistic security encompasses all of the functional units of a business enterprise: IT, human resources, legal, R&D, security, and many others. Such security is based on the premise that so-called “isolated incidents” occurring in one particular department should be juxtaposed with other data to: (a) corroborate the existence of possible vulnerabilities; and (b) help identify other negative trends. The following four examples demonstrate how various isolated incidents, when interpreted holistically, can help skilled investigators understand the nature of a possible threat directed against a company’s key value drivers.

***Isolated Incident No. 1.*** A member of a company’s IT Department observes Employee A trying to gain access to a folder for which the employee does not have permission to access. This folder contains sensitive information on a prototype development not yet introduced to the market. A week later, the same employee was found running a scan of the company’s internal network. When IT staff noticed this activity, they confronted the employee, who offered what the staff considered to be a plausible explanation. No subsequent action was taken; and the information was not shared with any other department within the company.

***Isolated Incident No. 2.*** The office manager has noticed Employee A working late hours – an irregular and seemingly unnecessary activity. Late one evening, Employee A attempted to leave the building with a bag containing folders labeled “proprietary.” When the office manager questioned the employee, the latter responded with a frantic apology and offered a plausible explanation. Accepting the response as legitimate, the office manager did not share this information with anyone else in the company.

***Isolated Incident No. 3.*** A different employee (Employee B) recently traveled overseas to attend a meeting with a foreign partner on a joint venture opportunity. During the trip, the employee traveled with not only his smartphone but also a company laptop – both of which contained proprietary information. Moreover, on more than one occasion, Employee B had accessed the U.S. company’s network from the joint venture partner’s internal network. Apparently not thinking anything of it, Employee B did not, after his return, mention those actions to any of his colleagues.

***Isolated Incident No. 4.*** At lunch on a Monday morning, colleagues learned that Employee A had just returned from a weekend trip overseas. When asked for details about the trip, the employee offered a hurried and somewhat confusing explanation about a “weekend getaway” that appeared to be in conflict with his/her established lifestyle pattern. Later that day, colleagues learned that Employee A had traveled with numerous company thumb-drives and disks – also rather unusual behavior for a traveler supposedly on a vacation. Moreover, over a longer period of time, colleagues started to notice some unexplained affluence on the part of Employee A – driving a brand new car, for example, rather than the more modest vehicle Employee A previously drove. When queried by a colleague, Employee A stated somewhat awkwardly that the car had been a gift from a distant relative. Without additional information confirming the suspicions already aroused, however, the issue was dropped; and the information already developed was not shared with anybody else inside the company.

**Share, Study, Assess, Confirm**

As individual data points, the preceding incidents may seem mundane and/or ordinary to those who witnessed the various actions mentioned. But if those incidents had been documented, and not only correlated but also analyzed with the information collected from the other departments, certain patterns might well have emerged that would confirm the incidents as potential evidence pointing to a targeted campaign to steal the company’s intellectual property.

In an era of increasingly sophisticated threats, the protection of intellectual assets may best be served through adoption of a holistic approach to security using both trusted intelligence methodologies and properly trained personnel. To do anything less, in fact, could have disastrous consequences. The failure “to address the challenge of trade secret theft costs industry billions of dollars each year,” said Pamela Passman, president and chief executive officer of CREATe.org, a leading nonprofit dedicated to helping companies, suppliers, and business partners reduce piracy, counterfeiting, and trade secret theft. Moreover, she added, such thefts “can have devastating reputational, financial, and legal impacts … [not only] for individual companies … [but also for] the global economy as a whole.”

***Armond Caglar*** *is a security solutions consultant at Tailored Solutions and Consulting (TSC), an enterprise risk consultancy based in Washington, D.C. Prior to establishing himself in his current position, he served in the U.S. government for more than seven years conducting worldwide operations in support of sensitive national-level priorities. He holds both a Master’s degree from Tufts University and a Bachelor of Arts degree from the University of New Hampshire.*

# How Would the U.S. Respond to a Nightmare Cyber Attack?

**By Josephine Wolff**

Source: http://www.scientificamerican.com/article.cfm?id=how-would-us-respond-nightmare-cyber-attack&&goback=.gde\_3904448\_member\_261655493

It’s been a busy summer for computer security mavens. The U.S. and China locked horns on cyber espionage, Edward Snowden allegedly leaked classified intelligence about National Security Agency (NSA) monitoring programs that target communication networks, and the Cobalt malware took 13 U.S. oil refineries offline. If you missed that last one, that’s because it was fictional—a scenario created for a student cyber attack challenge held on June 15 at American University in Washington, D.C.

The event was a sort of a hybrid Model U.N. hackathon cyber war games exercise, involving 65 college and graduate students (including myself) who are training for careers as future cyber warriors and policy makers. In many ways the Cyber 9/12 Student Challenge mirrors the U.S. government’s own Cyber Storm exercises, with the important exception that the student exercise isn’t mandated by Congress to strengthen cyber preparedness in the public and private sectors.

The Cobalt malware—an invention of the Atlantic Council, which hosted the event—was fake, but its target was a real-life vulnerability: the U.S. energy infrastructure, specifically the oil refineries and pipelines that produce and transport gasoline and other refined fuel products all across the country. Almost any discussion or description of a doomsday cyber scenario involves an attack on U.S. critical infrastructure. You can see this play out in the Cyber Storm exercises hosted every few years by the Department of Homeland Security for government and industry organizations to practice cyber threat responses. In three simulations that took place in 2006, 2008 and 2010, catastrophic cyber attacks caused clear and serious physical damage. A computer virus that turns off the lights, shuts down the telephone system and halts military operations could cost lives.

To date, intentional computer-based attacks that have direct physical impacts have been few and far between, so far as we know. That doesn’t mean these scenarios couldn’t happen in real life, or that there aren’t real and serious vulnerabilities in the country’s critical infrastructure networks. There is a perception that we haven’t yet experienced such a catastrophe because of a combination of luck and the reluctance on the part of nations, militias and other entities capable of launching a cyber attackto set a dangerous precedent. In 2011, for instance, news outlets reported that the Obama administration decided against infiltrating the computer systems of the Libyan government to interfere with their military communications and air-defense system due to concerns about whether other nations might follow suit as well as uncertainty surrounding whether such measures required Congressional approval. The Stuxnet worm that in 2010 struck Iranian nuclear facilities, causing centrifuges to speed up, thereby interrupting the uranium enrichment process essential for the development of nuclear technology, is the exception, judging by unclassified knowledge.

At the Atlantic Council’s event, there was a strong sense that a successful cyber attack on U.S. critical infrastructure is inevitable. There’s also a pervasive fear that when (or if) such an attack occurs, the U.S. is primed to overreact. Department of Defense announcements that they intend to view cyber attacks as “acts of war” suggest a military force nearly itching to flex its muscle in response to a serious computer network–based disruption, if only as a means of deterrence. Cybersecurity professionals—not to mention students hoping to work in the field someday—can also have an incentive to trumpet the threat of cyber attack that at times may heighten the risk of overreaction. At least five times over the course of the daylong cyber challenge, we were reminded by presiding officials how crucially important the work we’re doing is, and how desperately the country needs people like us.

Concerns about overreaction and the use of military force in response to digital intrusions often lead to discussions about the difficulty surrounding definitive attribution of these types of attack. If you want to retaliate, how do you know whom to hit? In our exercise intelligence pointed to Russia, but the evidence wasn’t clear-cut.

Most teams urged against retaliating in kind with a comparable cyber attack or to exercising traditional military power. Cobalt was not devastating, and Russia was not clearly the culprit. Several groups advocated diplomatic engagement, echoing the approach taken by the actual U.S. government just one week earlier during the informal summit between President Obama and Chinese leader Xi Jinping in Rancho Mirage, Calif., where cyber espionage was among the topics discussed.

But, again, espionage is not the nightmare scenario—nor is the shutdown of 13 oil refineries. Still, halfway through the student competition in Washington, D.C., when the scenario was updated with new (fake) intelligence indicating a severe escalation of the Cobalt situation, policy recommendations began to veer more toward displays of cyber and physical force by the U.S. military.

The update was alarming: three oil pipelines in the Gulf coast region had been shut down, following malfunctions, and several other pipelines in the region were taken off-line to search for Cobalt infections. Meanwhile, supervisory control and data acquisition system vendors in the U.S. and Germany were experiencing a distributed denial-of-service (DDoS) attack, and several terminals and servers in Russia had been identified as responsible for both the DDoS attacks and activation of the Cobalt malware. The stock market was dropping like a rock, and several private sector firms appeared poised to carry out their own form of vigilante retaliation against Russia by trying to identify and penetrate or cut off the responsible parties’ servers and networks.

The teams had to come up with a response to this escalation within hours. The time pressure was intense, and as the situation grew more serious, the consensus for diplomatic engagement dissolved. The 19 groups suddenly diverged considerably about what the proper response should be. The 65 students, all in their mid- to late 20s, wearing business suits and military uniforms, filled every open classroom in the American University’s School of International Service, whispering feverishly about whether the U.S. should launch a DDoS attack of its own, bomb the Kremlin, invoke Article 5 of NATO to set in motion a collective defense by U.S. allies, or to authorize the members of the private sector to exact their own revenge by working among themselves to shut off connectivity to pieces of the network carrying malicious traffic or to infiltrate or flood the responsible servers.

What does this say about how the U.S. government would respond to such a situation? The recent cases of high-volume espionage of China, which are considerably less intrusive than the fictional Cobalt attacks, don’t give us much to go on. Would the U.S. stick to diplomacy or turn bellicose?

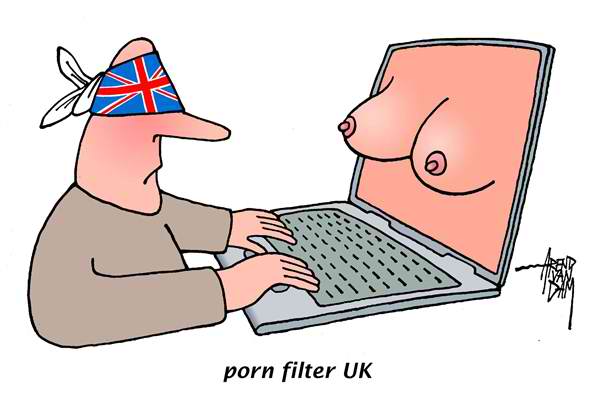
The more important question is how well prepared will the U.S. be if and when an attack comes? Considering how a cyber attack would play out in the heat of the moment may be more exciting than the reality, because by the time an attack occurs many of the options may be practically preordained by the security controls we have in place. Preparation determines the quality, agility and sophistication of answers to mundane but important questions: What kinds of security standards are in place for critical infrastructure networks? Who sets them? Who enforces them? What threat information do companies and government agencies share with one another? How do they share this data—and how quickly? The ability to answer these questions will ultimately determine the impact of a large-scale, sophisticated computer network breach. And because the Pentagon has asserted that its response will be commensurate to the impact of an attack, rather than the means, how effectively we prepare will play a major role in influencing what our response ultimately looks like.

We may soon know what the U.S. government would do. Many people in the field are expecting to see a major breach soon. As former CIA and NSA director Michael Hayden predicted in his keynote remarks to the students at the cyber challenge, “By the time you do this next year, you won’t have to be so imaginative in creating the scenario.”

***Josephine Wolff*** *is a PhD candidate in the Engineering Systems Division at Massachusetts Institute of Technology studying cybersecurity and Internet policy.*

# UK 'Porn' Filter Will Also Block Violence, Alcohol, Terrorism, Smoking and 'Esoteric Material'

Source:http://www.huffingtonpost.com/2013/07/29/uk-internet-filter-block-more-than-porn\_n\_3670771. html?ncid=edlinkusaolp00000003

The United Kingdom's new internet filters promise to block much more than just pornography, according to a report by the digital advocacy organization Open Rights Group.

Last week, Prime Minister David Cameron announced online porn would soon become automatically blocked in order to "protect children and their innocence." The filters will be implemented by the UK's major internet service providers, which encompass 95% of British web users.

Based on conversations with several ISPs, Open Rights Group says the new "parental controls" will reach far beyond pornography. By default, the controls will block access to "violent material," "extremist and terrorist related content," "anorexia and eating disorder websites," and "suicide related websites."

In addition, the new settings will censor websites that mention alcohol or smoking. The filter will even block "web forums" and "esoteric material," though Open Rights Group does not specify what these categories would include.

The Independent notes the filters implemented by the four main private internet providers will be "default-on," meaning users must explicitly choose to turn them off. Users can decide to keep certain filters while turning others off.

Making the filters default means most people will keep them, according to Open Rights Group Executive Director Jim Killock. "We know that people stick with defaults: this is part of the idea behind 'nudge theory' and 'choice architecture' that is popular with Cameron."

According to Cameron, the new parental control settings will be turned on for all new broadband subscribers "by the end of the year."

ONLINE DEBATE: Cyber-warfare – Is the risk of cyber-warfare overrated?

Source: http://www.economist.com/debate/days/view/999?fsrc=scn/tw/te/db/cl/cyberwarfare

|  |
| --- |
| **Closing statements** |

|  |  |
| --- | --- |
| **Defending the motion**  Thomas Rid  *Thomas RidReader in War Studies, King's College London*  The real question is whether the internet will remain free as in most democratic countries today, or whether it will be heavily restricted and supervised, as in many authoritarian regimes today | Richard Bejtlich  **Against the motion**  Richard Bejtlich  *Chief Security Officer, Mandiant*  An executive order from President Obama states: "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." This is not rhetoric. |

|  |
| --- |
| **Edward LucasThe moderator's closing remarks**  Jul 31st 2013 | Edward Lucas  First of all, thanks to both our contributors and to the many who have commented. I don't know if it was just coincidence that our website went down on Tuesday: certainly it was a reminder of the fragility of cyber-normality.  I am glad we moved away from the questions of semantics. These are important, but the real question is what actions we take, not what words we use to describe them. (I come from a culture where a savage career-ending rebuke can be delivered with the words: "I was a bit disappointed to learn…")  Richard Bejtlich (writing from the Black Hat hackfest) has highlighted the "watershed" pronouncement from America's Securities and Exchange Commission (SEC) which moves cyber-security from the IT cubicle to the boardroom. It is now under a legal duty to disclose attacks (though to what level of detail remains to be seen). President Obama's executive order in February has increased the obligations for those who protect the nation's critical infrastructure.  But we need to do more, Mr Bejtlich argues. Attacks are inevitable: the question is how quickly we identify them and how we respond—by mitigating their effects (or as he doesn't say, but many would) by counter-attacking.  Earlier, he had argued that we must learn from the way that our enemies (such as China's People's Liberation Army) use language. If they think warfare involves non-violent use of information, we should arrange our defences accordingly. Thomas Rid disagrees: why should we "bow to the twisted logic of these Chinese writers", he asks. We don't lock up our dissidents or engage (pace Edward Snowden) in mass-surveillance. We need not a cruder view, he argues, but more nuance.  That would mean appreciating that cyberspace, like real life, is full of conflicts. We need to identify them, but not necessarily to use military rhetoric to win them at all costs. The real goal is not victory over adversaries, be they Chinese, Iranian, Russian or our own domestic cyber-criminals. The real goal is to maintain the "normal" internet. If so, Mr Rid argues, "calling for PLA-inspired emergency rules in cyberspace risks making the problem worse."  I appreciated the comment by Pramutka, who made three interesting points. One is that compromising information flow could be a prelude to war. That reminds me of the old law of the sea, in which a naval blockade is an act of war. The dangers of escalation deserve a lot more scrutiny: what are the circumstances in which a cyber-attack could or should bring a "kinetic" response (or, theoretically I suppose, vice versa). What kinds of "red lines" can countries reasonably draw in cyberspace and what level of attribution do we need before we launch a response (the question of automatic retaliation adds an extra level of danger and complexity). Pramutka also raises the question of whether explicitly counting espionage, sabotage, and subversion as "not war" lowers the cost of launching them.  His third point is about public-private tensions. The assumption so far is that governments either help their businesses or leave them alone. But the National Security Agency revelations from Mr Snowden have highlighted another dimension: what about companies that are under a legal duty to help their government (perhaps in placing backdoors and trapdoors in hardware and software) in a way which, if it comes to light, will be devastating for their business models? In such cases, the demands of economic warfare and cyberwar would clash.  Readers who have not voted are strongly encouraged to do so. And there is still time for some closing comments. |

|  |  |
| --- | --- |
| Thomas Rid  **The proposer's closing remarks**  Jul 31st 2013 | Thomas Rid  Is the risk of cyberwar overrated? The answer, as several readers have pointed out, indeed hinges on terminology. But the argument—talk of cyberwar is wrong—is not just semantic. Language matters. Language frames ideas. And ideas are powerful: ideas determine how we see the problem, what we do to solve it, who we think should be in charge, and how governments spend taxpayers' money.  Analogies can deceive. Real war is hellish: men kill other men, women get raped, and children die for no reason. News from Syria, Iraq and Afghanistan is an almost daily reminder that "cyberwar" remains a metaphor—just like the "war on cancer" and the "war on drugs", except that these are much more dangerous for the people involved. The crux is that metaphors and analogies break down at some point, and it is crucial to recognise that point of breakdown. Missing it means we may be fooling ourselves.  Richard Bejtlich turns to the People's Liberation Army of China for help. Chinese thinkers, he says, understand that war can be violent or non-violent, that it can be a confrontation between soldiers or between ordinary people or "experts". Mr Bejtlich approvingly quotes Qiao Liang and Wang Xiangsui to make the point that "the battlefield is everywhere". I'm less willing to bow to the twisted logic of these Chinese writers. China engages in practices that free societies are explicitly unwilling to accept, such as mass surveillance, rounding up dissidents and state-sponsored economic espionage. So PLA strategists are not right automatically, nor should they be able to dictate how we see the problem. What we need is not an even cruder view, but more nuance.  More nuance means recognising that talk of the enemy is misplaced. China is only part of the problem. Other actors are equally exploiting insecure software and vulnerable computer networks. These include eastern European criminals, some companies, anonymous activists, militants of all stripes, the Iranian military and spy agencies everywhere, including in Russia, America and Europe. Some of these activities are lawful and legitimate, others are illegal and unjustified. The fine line in between cannot be drawn with a broad brush borrowed from the PLA.  More nuance means understanding that talk of "cyberwar" may be in the interest of those with a harsher vision of the web's future. There is not one "intensive and open-ended nation-state conflict over the control of cyberspace", as one reader pointed out—there are many such conflicts. Countries take control over their cyberspace, over their sovereign corner of the internet. Non-democracies are tempted to tweak their national technical infrastructures, their national laws and their firewalls to "protect their sovereignty in cyberspace"—which in practice means protecting intellectual property thieves from foreign pressure and arresting political activists at home.  More nuance, finally, means seeing the true challenge. The real question is what the "normal" internet experience is today, and will be in the future: whether the internet will remain free, as in most democratic countries today, or whether it will be heavily restricted and supervised, as in many authoritarian regimes today. If "normal" is measured by the numbers, the future of freedom already looks bleak. Calling for PLA-inspired emergency rules in cyberspace risks making the problem worse.  "Cyberwar", Mr Bejtlich concedes, "will be far less violent." But then he compares less-violent computer attack to the extraordinarily violent use of air power in the second world war. That comparison may be confusing at first glance. But it brings one question into sharp relief: should the air force, or the armed forces more generally, be in charge of this type of non-violent conflict where the battlefield is "everywhere"?  No. We need the armed forces to stay focused on fighting and winning the real wars of the future. That's hard enough. Let us not militarise the struggle for the free and liberal internet today. | Richard Bejtlich  **The opposition's closing remarks**  Jul 31st 2013 | Richard Bejtlich  Our moderator requested we pivot from discussing cyberwar to addressing "questions of resilience and vulnerability" and "how and whether modern societies can cope with them", ultimately asking if "the threat [is] so severe that we need new rules for dealing with it". This response to the moderator's request shows that risks in the cyber-environment are real and increasing. Three examples are relevant.  First, in October 2011, the Securities and Exchange Commission (SEC) issued "CF [Corporate Finance] Disclosure Guidance: Topic No. 2", clarifying the requirements facing publicly traded companies with respect to cyber-security. The SEC statement outlined "specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents". This watershed pronouncement moved the discussion of "cyber" from the IT cubical to the boardroom. Following the guidance, the SEC pressed companies for details on digital incidents; many are now posted on its website.  Second, in February 2013, President Obama issued an executive order titled "Improving Critical Infrastructure Cybersecurity", stating: "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." This is not rhetoric: the government's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to more than 200 incidents between October 2012 and May 2013, compared with only nine in all of 2009. Insiders claim that a speech by the former defence secretary, Leon Panetta, on cyber-security in October 2012 was a warning to those attacking American critical infrastructure.  Third, the number of countries transitioning from "digital nuisances" to real threats is growing. Although states like Russia and China have long histories as sources of nation-state and "patriotic" hacking, new actors are reaching the top league. Iran is the suspected perpetrator of an August 2012 digital attack against Saudi Aramco that rendered over 30,000 of its computers useless. Analysts also believe Iran continued its assault by hitting Qatar-based RasGas a few days later. Besides Iran, security professionals now worry about North Korea, which conducted a similar "sabotage" operation against South Korea in March 2013 that corrupted over 32,000 computers. These episodes of mass digital sabotage are unprecedented and risk causing damage beyond that anticipated by attacker or victim.  I write this statement while attending the world's premier security conference, Black Hat. Researchers deliver talks with titles like "Exploiting Software Running on Three Billion Devices", "Breaking Home Security Systems and Bypassing Building Controls", "Energy Fraud and Orchestrated Blackouts", "Compromising Industrial Facilities from 40 Miles Away" and "Implantable Medical Devices: Hacking Humans". I first attended the conference in 2002, and the attention now paid to systems which truly matter – industrial control, home security, medicine – is staggering. These are open discussions by responsible parties, unlike those in the underground economy or in the war rooms of disgruntled powers. Spend any amount of time in this environment, with the people figuring out how cyberwar really works, and you will be astonished. Furthermore, top policymakers and leaders are present: the director of the National Security Agency, Keith Alexander, is the keynote speaker.  How can we cope? Are new rules needed? The model I promote in my new book, "The Practice of Network Security Monitoring", emphasises precise threat detection, rapid incident response and thorough threat containment. We need to abandon plans that rely on keeping all intruders out of the network. Instead, we should expect intrusions, but quickly remove attackers once we discover that they have breached our defences. These are truly the "new rules" which can reduce the risk of damage caused by digital attacks and cyberwar. |

***Thomas Rid*** *is a Reader in War Studies at King's College London. Before that he was a visiting scholar at the Hebrew University and the Shalem Centre in Jerusalem. From 2006 to 2009 he worked at the School for Advanced International Studies, Johns Hopkins University, the RAND Corporation in Washington, DC, and the Institut français des relations internationales in Paris. He wrote his first book at the Stiftung Wissenschaft und Politik, Berlin's major foreign policy think-tank. He is the author of "Cyber War Will Not Take Place" (Oxford University Press/Hurst), "Understanding Counterinsurgency" (co-edited with Tom Keaney, Routledge, 2010), "War 2.0" (with Marc Hecker, Praeger, 2009, and in Chinese by the People's Liberation Army Press, 2011) and "War and Media Operations" (Routledge, 2007). His numerous articles have appeared in various and German peer-reviewed journals as well as magazines and newspapers.*

***Richard Bejtlich*** *is chief security officer at Mandiant, a cyber-security firm. He has more than 15 years' experience in enterprise-level intrusion detection and incident response. Before joining Mandiant, he was director of incident response at General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Earlier, he operated TaoSecurity as an independent consultant, protected national security interests for ManTech Corporation's Computer Forensics and Intrusion Analysis division, investigated intrusions as part of Foundstone's incident-response team and monitored client networks for Ball Corporation. He began his digital-security career as a military intelligence officer at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Centre (AFIWC) and Air Intelligence Agency (AIA). He is the author of "The Tao of Network Security Monitoring" and "Extrusion Detection", and co-author of "Real Digital Forensics". He currently writes a blog, taosecurity.blogspot.com, and teaches for Black Hat.*

***Edward Lucas*** *is the international section editor at* The Economist*; he has also covered the central and east European region for over 25 years. His postings included stringing for* The Economist *in communist-era Czechoslovakia and later in the Baltic states, as well as being editorial director of the Economist Intelligence Unit in Vienna. In 1996 he became Berlin correspondent and in 1998 Moscow bureau chief. After leaving Russia in 2002, he covered education and transport for the Britain section until 2005. Since then he has worked on the international section, which he now edits. He is the author of "Deception", a book about Russian espionage, published in March 2012. His first book was the "The New Cold War", published in February 2008. He is currently working on a book on the politics of cyber-security.*

# Can cars be hacked?

Source: http://i-hls.com/2013/07/can-cars-be-hacked/?goback=.gde\_4709642\_member\_259807163

**In the early hours of  June 18th, a Mercedes coupé travelling at an extremely high speed along a Los Angeles street smashed into a palm tree. It exploded into flames, killing the driver; the impact ejected the engine 50 meters clear of the car. Was it an accident? Or was the car hacked, allowing it to be driven off the road by remote control?**

**According to New Scientist the very idea might sound like a scene from a Hollywood blockbuster but it’s one that Richard Clarke, a former counterterrorism adviser to the US National Security Council, has raised after the driver was identified as *Rolling Stone* journalist Michael Hastings. Known for his revealing articles on the US military and its intelligence agencies, Hastings had emailed colleagues the day before he died to say that he was going “off the radar for a bit” to chase down a “big story”.**

“The evidence publically available is consistent with a car CYBER attack” says Clarke in a *Huffington Post* interview. Intelligence agencies, he says, can remotely seize control of a car to make it accelerate wildly or brake suddenly, for instance.

Clarke cited research, carried out for the US National Academy of Sciences, showing that “connected cars” – equipped with built-in cellular technology used by dashboard apps and engine-monitoring software – can be hacked remotely. But practical proof has been lacking.

That looks set to change on July 27th, when Spanish engineers Javier Vázquez Vidal and Alberto Garcia Illera will give a demonstration at the Black Hat security conference in Las Vegas, Nevada. They have built a $25 device that lets them bypass security in a car’s electronic control unit.

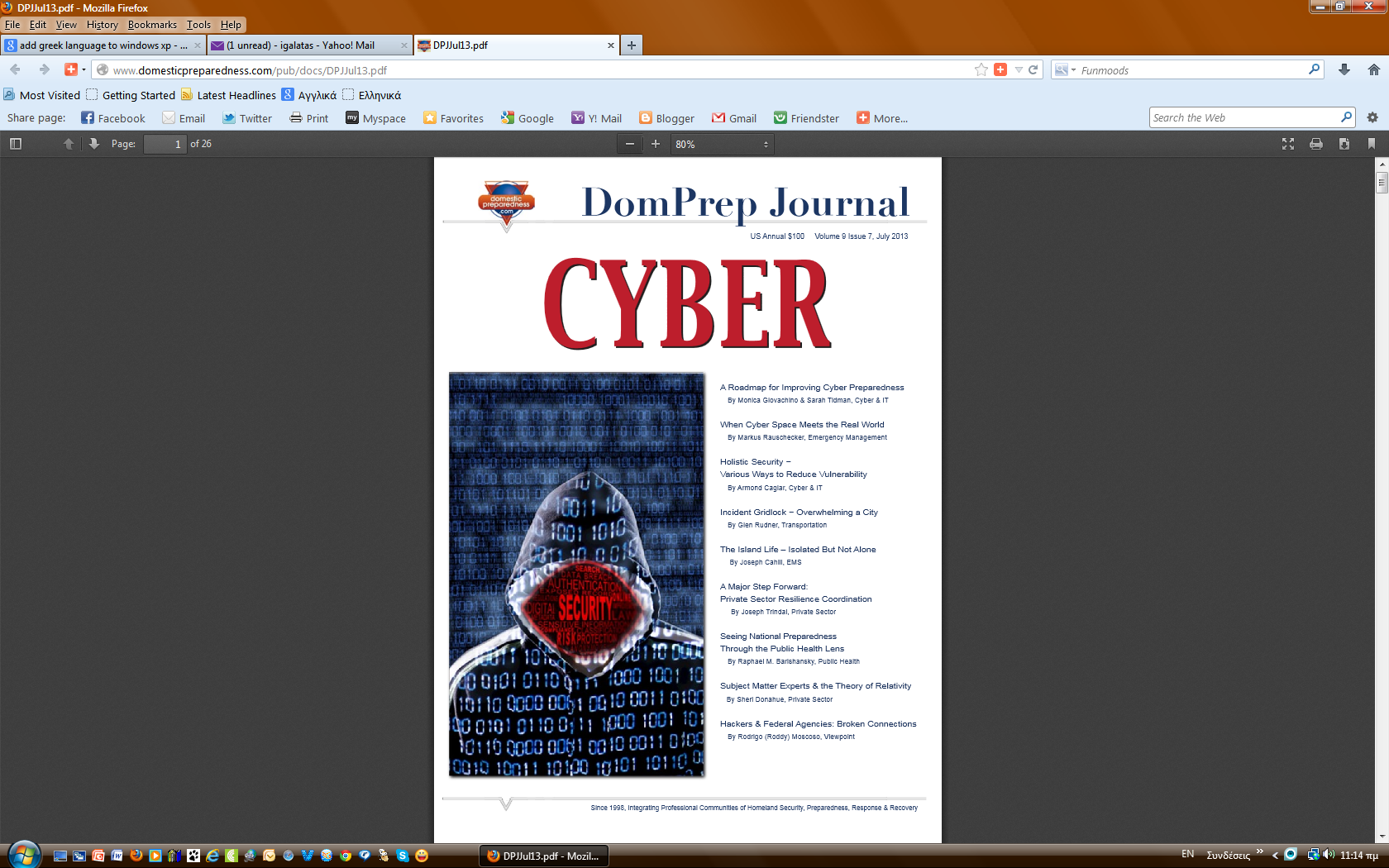
The brain of a modern car, the ECU, is a computer that controls engine power, transmission and braking. Mechanics can diagnose faults by plugging a laptop into it via standard wired connectors such as the CAN bus. Alternatively, remote diagnostics and software updates can take place over a cellular network, as happens with services such as General Motors’ OnStar and Mercedes-Benz’s Mbrace.

Vázquez Vidal and Garcia Illera will show how their device – which they claim uses a $1 chip to break encryption – can read from and write data to the flash memory of commonly used ECUs, made by Bosch of Germany. In this way, they can get more horsepower out of a car, or tell it to burn less fuel. “And it would take no time to gain total control over a vehicle – deploying an airbag, activating the brakes, or immobilizing a car at any moment,” says Vázquez Vidal.

How they have done this is unclear. “My best guess is that they have managed to put the ECU into an unencrypted test state, possibly by playing around with power-up sequences,” says Peter Highton, a senior engineer with Freescale Semiconductor in Aylesbury, UK, which makes ECU microchips for racing cars as well as ordinary vehicles.

For security, connected cars should use encryption, but Highton says carmakers are only just coming to terms with it. “Until as recently as five years ago, data on the CAN bus of most cars was unencrypted, and so could be intercepted and altered.”

Whatever the causes of Michael Hastings’s crash, the need to make cars secure against hacking will only become more acute. The next version of Vázquez Vidal and Garcia Illera’s device won’t even need plugging in to the target car. “I am already working on a wireless version,” Vázquez Vidal says.



# XKeyscore mapXKeyscore

Source: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

One presentation claims the XKeyscore program covers 'nearly everything a typical user does on the internet'

A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden.

The NSA boasts in training materials that the program, called XKeyscore, is its "widest-reaching" system for developing intelligence from the internet.

The latest revelations will add to the intense public and congressional debate around the extent of NSA surveillance programs. They come as senior intelligence officials testify to the Senate judiciary committee on Wednesday, releasing classified documents in response to the Guardian's earlier stories on bulk collection of phone records and Fisa surveillance court oversight.

The files shed light on one of Snowden's most controversial statements, made in his first video interview published by the Guardian on June 10.

"I, sitting at my desk," said Snowden, could "wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email".

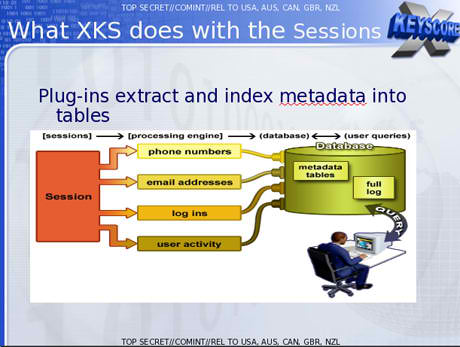
US officials vehemently denied this specific claim. Mike Rogers, the Republican chairman of the House intelligence committee, said of Snowden's assertion: "He's lying. It's impossible for him to do what he was saying he could do."

But training materials for XKeyscore detail how analysts can use it and other systems to mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search. The request is not reviewed by a court or any NSA personnel before it is processed.

XKeyscore, the documents boast, is the NSA's "widest reaching" system developing intelligence from computer networks – what the agency calls Digital Network Intelligence (DNI). One presentation claims the program covers "nearly everything a typical user does on the internet", including the content of emails, websites visited and searches, as well as their metadata.

Analysts can also use XKeyscore and other NSA systems to obtain ongoing "real-time" interception of an individual's internet activity.

Under US law, the NSA is required to obtain an individualized Fisa warrant only if the target of their surveillance is a 'US person', though no such warrant is required for intercepting the communications of Americans with foreign targets. But XKeyscore provides the technological capability, if not the legal authority, to target even US persons for extensive electronic surveillance without a warrant provided that some identifying information, such as their email or IP address, is known to the analyst.

One training slide illustrates the digital activity constantly being collected by XKeyscore and the analyst's ability to query the databases at any time.

The purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email account (a "selector" in NSA parlance) associated with the individual being targeted.

Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used.

One document notes that this is because "strong selection [search by email address] itself gives us only a very limited capability" because "a large amount of time spent on the web is performing actions that are anonymous."

The NSA documents assert that by 2008, 300 terrorists had been captured using intelligence from XKeyscore.

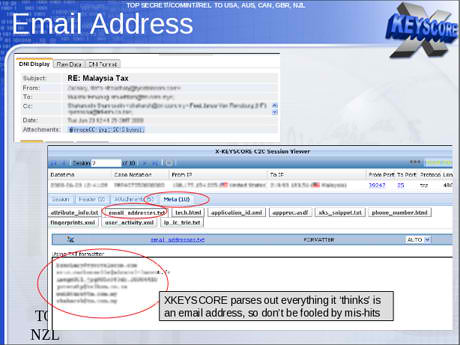
Analysts are warned that searching the full database for content will yield too many results to sift through. Instead they are advised to use the metadata also stored in the databases to narrow down what to review.

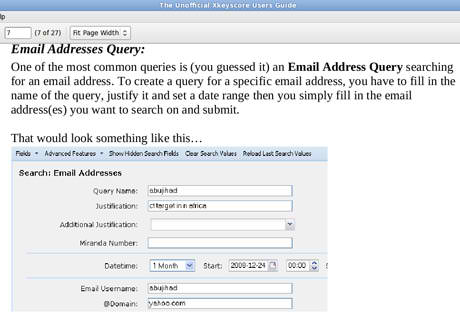
A slide entitled "plug-ins" in a December 2012 document describes the various fields of information that can be searched. It includes "every email address seen in a session by both username and domain", "every phone number seen in a session (eg address book entries or signature block)" and user activity – "the webmail and chat activity to include username, buddylist, machine specific cookies etc".

## Email monitoring

In a second Guardian interview in June, Snowden elaborated on his statement about being able to read any individual's email if he had their email address. He said the claim was based in part on the email search capabilities of XKeyscore, which Snowden says he was authorized to use while working as a Booz Allen contractor for the NSA.

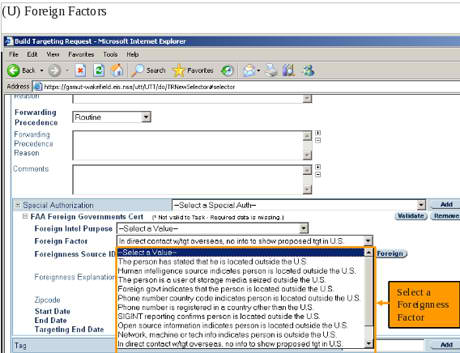
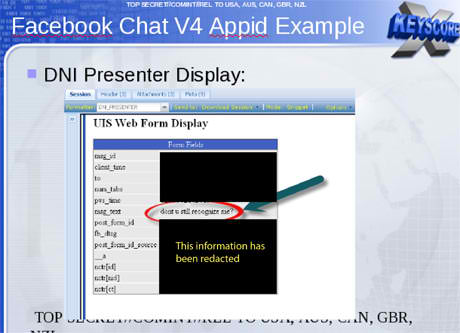
One top-secret document describes how the program "searches within bodies of emails, webpages and documents", including the "To, From, CC, BCC lines" and the 'Contact Us' pages on websites".

To search for emails, an analyst using XKS enters the individual's email address into a simple online search form, along with the "justification" for the search and the time period for which the emails are sought.



The analyst then selects which of those returned emails they want to read by opening them in NSA reading software.

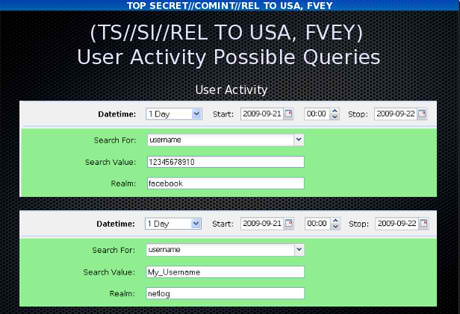
The system is similar to the way in which NSA analysts generally can intercept the communications of anyone they select, including, as one NSA document put it, "communications that transit the United States and communications that terminate in the United States".

One document, a top secret 2010 guide describing the training received by NSA analysts for general surveillance under the Fisa Amendments Act of 2008, explains that analysts can begin surveillance on anyone by clicking a few simple pull-down menus designed to provide both legal and targeting justifications. Once options on the pull-down menus are selected, their target is marked for electronic surveillance and the analyst is able to review the content of their communications:

## Chats, browsing history and other internet activity

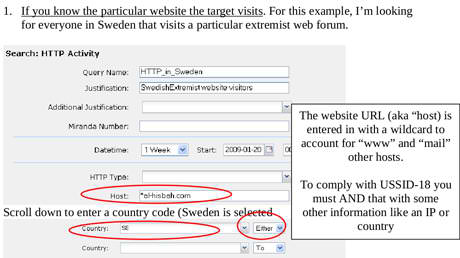
Beyond emails, the XKeyscore system allows analysts to monitor a virtually unlimited array of other internet activities, including those within social media.

An NSA tool called DNI Presenter, used to read the content of stored emails, also enables an analyst using XKeyscore to read the content of Facebook chats or private messages.

An analyst can monitor such Facebook chats by entering the Facebook user name and a date range into a simple search screen.

Analysts can search for internet browsing activities using a wide range of information, including search terms entered by the user or the websites viewed.

As one slide indicates, the ability to search HTTP activity by keyword permits the analyst access to what the NSA calls "nearly everything a typical user does on the internet".

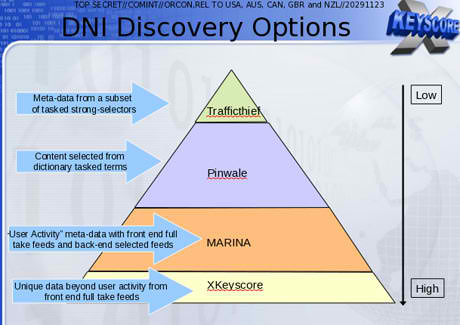
The XKeyscore program also allows an analyst to learn the IP addresses of every person who visits any website the analyst specifies.

The quantity of communications accessible through programs such as XKeyscore is staggeringly large. One NSA report from 2007 estimated that there were 850bn "call events" collected and stored in the NSA databases, and close to 150bn internet records. Each day, the document says, 1-2bn records were added.

William Binney, a former NSA mathematician, said last year that the agency had "assembled on the order of 20tn transactions about US citizens with other US citizens", an estimate, he said, that "only was involving phone calls and emails". A 2010 Washington Post article reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications."

The XKeyscore system is continuously collecting so much internet data that it can be stored only for short periods of time. Content remains on the system for only three to five days, while metadata is stored for 30 days. One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."

To solve this problem, the NSA has created a multi-tiered system that allows analysts to store "interesting" content in other databases, such as one named Pinwale which can store material for up to five years.

It is the databases of XKeyscore, one document shows, that now contain the greatest amount of communications data collected by the NSA.

In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.

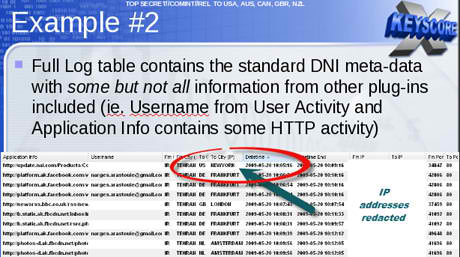
**Legal v technical restrictions**

While the Fisa Amendments Act of 2008 requires an individualized warrant for the targeting of US persons, NSA analysts are permitted to intercept the communications of such individuals without a warrant if they are in contact with one of the NSA's foreign targets.

The ACLU's deputy legal director, Jameel Jaffer, told the Guardian last month that national security officials expressly said that a primary purpose of the new law was to enable them to collect large amounts of Americans' communications without individualized warrants.

"The government doesn't need to 'target' Americans in order to collect huge volumes of their communications," said Jaffer. "The government inevitably sweeps up the communications of many Americans" when targeting foreign nationals for surveillance.

An example is provided by one XKeyscore document showing an NSA target in Tehran communicating with people in Frankfurt, Amsterdam and New York.

In recent years, the NSA has attempted to segregate exclusively domestic US communications in separate databases. But even NSA documents acknowledge that such efforts are imperfect, as even purely domestic communications can travel on foreign systems, and NSA tools are sometimes unable to identify the national origins of communications.

Moreover, all communications between Americans and someone on foreign soil are included in the same databases as foreign-to-foreign communications, making them readily searchable without warrants.

Some searches conducted by NSA analysts are periodically reviewed by their supervisors within the NSA. "It's very rare to be questioned on our searches," Snowden told the Guardian in June, "and even when we are, it's usually along the lines of: 'let's bulk up the justification'."

In a letter this week to senator Ron Wyden, director of national intelligence James Clapper acknowledged that NSA analysts have exceeded even legal limits as interpreted by the NSA in domestic surveillance.

Acknowledging what he called "a number of compliance problems", Clapper attributed them to "human error" or "highly sophisticated technology issues" rather than "bad faith".

However, Wyden said on the Senate floor on Tuesday: "These violations are more serious than those stated by the intelligence community, and are troubling."

In a statement to the Guardian, the NSA said: "NSA's activities are focused and specifically deployed against – and only against – legitimate foreign intelligence targets in response to requirements that our leaders need for information necessary to protect our nation and its interests.

"XKeyscore is used as a part of NSA's lawful foreign signals intelligence collection system.

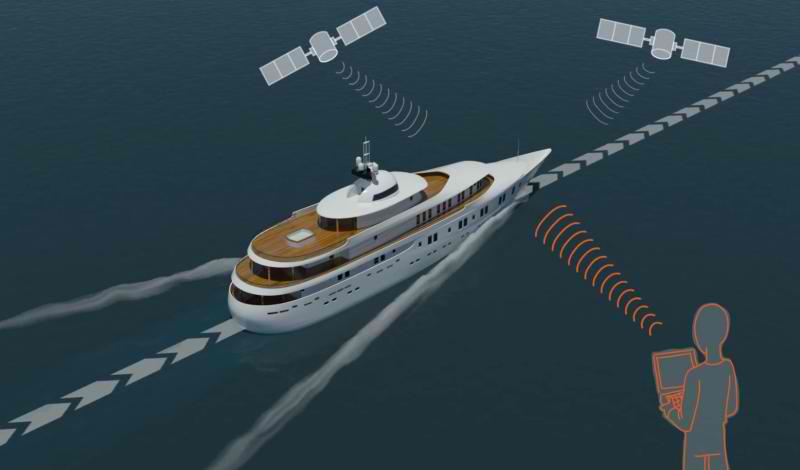
"Allegations of widespread, unchecked analyst access to NSA collection data are simply not true. Access to XKeyscore, as well as all of NSA's analytic tools, is limited to only those personnel who require access for their assigned tasks … In addition, there are multiple technical, manual and supervisory checks and balances within the system to prevent deliberate misuse from occurring."

"Every search by an NSA analyst is fully auditable, to ensure that they are proper and within the law.

"These types of programs allow us to collect the information that enables us to perform our missions successfully – to defend the nation and to protect US and allied troops abroad."

## Researchers successfully spoof an $80 million yacht at sea

Source: http://www.homelandsecuritynewswire.com/dr20130802-researchers-successfully-spoof-an-80-million-yacht-at-sea

This summer, a radio navigation research team from the University of Texas at Austin set out to discover whether they could subtly coerce a 213-foot yacht off its course, using a custom-made GPS device.

Led by assistant professor Todd Humphreys of the Department of Aerospace Engineering and Engineering Mechanics at the Cockrell School of Engineering, the team was able successfully to spoof an $80 million private yacht using the world’s first openly acknowledged GPS spoofing device. Spoofing is a technique that creates false civil GPS signals to gain control of a vessel’s GPS receivers. The purpose of the experiment was to measure the difficulty of carrying out a spoofing attack at sea and to determine how easily sensors in the ship’s command room could identify the threat.

A UT Austin release reports that the researchers hope their demonstration will shed light on the perils of navigation attacks, serving as evidence that spoofing is a serious threat to marine vessels and other forms of transportation. Last year, Humphreys and a group of students led the first public capture of a GPS-guided unmanned aerial vehicle (UAV), or drone, using a GPS device created by Humphreys and his students.

“With 90 percent of the world’s freight moving across the seas and a great deal of the world’s human transportation going across the skies, we have to gain a better understanding of the broader implications of GPS spoofing,” Humphreys said. “I didn’t know, until we performed this experiment, just how possible it is to spoof a marine vessel and how difficult it is to detect this attack.”

In June, the team was invited aboard the yacht, called the White Rose of Drachs, while it traveled from Monaco to Rhodes, Greece, on the Mediterranean Sea. The experiment took place about thirty miles off the coast of Italy as the yacht sailed in international waters.

From the White Rose’s upper deck, graduate students Jahshan Bhatti and Ken Pesyna broadcasted a faint ensemble of civil GPS signals from their spoofing device — a blue box about the size of a briefcase — toward the ship’s two GPS antennas. The team’s counterfeit signals slowly overpowered the authentic GPS signals until they ultimately obtained control of the ship’s navigation system.

Unlike GPS signal blocking or jamming, spoofing triggers no alarms on the ship’s navigation equipment. To the ship’s GPS devices, the team’s false signals were indistinguishable from authentic signals, allowing the spoofing attack to happen covertly.

The release notes that once control of the ship’s navigation system was gained, the team’s strategy was to coerce the ship onto a new course using subtle maneuvers that positioned the yacht a few degrees off its original course. Once a location discrepancy was reported by the ship’s navigation system, the crew initiated a course correction. In reality, each course correction was setting the ship slightly off its course line. Inside the yacht’s command room, an electronic chart showed its progress along a fixed line, but in its wake there was a pronounced curve showing that the ship had turned.

“The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line,” Humphreys said.

After several such maneuvers, the yacht had been tricked onto a parallel track hundreds of meters from its intended one — the team had successfully spoofed the ship.

The experiment helps illustrate the wide gap between the capabilities of spoofing devices and what the transportation industry’s technology can detect, Humphreys said.

Chandra Bhat, director of the Center for Transportation Research at the University of Texas at Austin, believes that the experiment highlights the vulnerability of the transportation sector to such attacks.

“The surprising ease with which Todd and his team were able to control a (multimillion) dollar yacht is evidence that we must invest much more in securing our transportation systems against potential spoofing,” Bhat said.

It is important for the public and policymakers to understand that spoofing poses a threat that has far-reaching implications for transportation, Humphreys said.

“This experiment is applicable to other semi-autonomous vehicles, such as aircraft, which are now operated, in part, by autopilot systems,” Humphreys said. “We’ve got to put on our thinking caps and see what we can do to solve this threat quickly.”

As part of an ongoing research project, funding and travel expenses for this experiment was supported by UT Austin’s Wireless Networking and Communications Group through the WNCG’s Industrial Affiliates program.

**Chinese hackers target remote conferencing gear**

Source: http://gadgets.ndtv.com/internet/news/chinese-hackers-target-remote-conferencing-gear-399900

A Chinese hacking group tied to the breach of security company RSA two years ago has targeted a maker of audio-visual conference equipment in a likely attempt to tap into boardroom and other high-level remote meetings.

Security researchers at Dell Inc's SecureWorks unit were able to monitor the computers used by the group to process communications from machines infected with stealthy software for stealing data, according to a paper they are releasing today.

Although the researchers could not tell what information was being extracted, they were able to discover many of the companies and offices unknowingly transmitting information. The compromised computers were in five different offices of a global maker of conferencing equipment, said SecureWorks researchers Joe Stewart and Don Jackson.

"I think they were looking for the source code," Stewart told Reuters, because that would help them find flaws they could use to eavesdrop in further attacks.

"If your final target is this vendor's customers of the conferencing product, you would want to be able to connect on their premises."

Stewart declined to identify the manufacturer, but he has notified both the company and law enforcement. Researchers had previously found security flaws in high-end conferencing gear and the new findings suggest they are a prime target.

As a hacking strategy, such a multi-step effort would track with other major attacks, including the one on RSA, a unit of EMC Corp.

In that case, the hackers took information that helped them duplicate the rapidly changing passwords on SecurID tokens used by defense contractors and others to authenticate users when they log in remotely. The contractors were the real targets in that case, researcher said.

Stewart attributed the new round of attacks to a prolific group based in Beijing that he and others have studied for years. Stewart's paper with Jackson tracks only one of the three dozen sophisticated malicious software programs that group favors.

That one family of code has hundreds of variants and has been used in at least 64 campaigns, including the penetration of the audio-visual equipment company, Stewart said. The same program has been used against government offices and 10 industries, including mining, media and communications.

Of the infections the researchers were able to identify, the greatest numbers were in Japan, followed by India, South Korea, Taiwan and the United States.

Stewart said the Beijing group is probably as big as the Shanghai-based crew that drew wide attention in February after security firm Mandiant said it was a specific unit within China's People's Liberation Army. China disputed the report and said it does not hack Western companies.

Although characteristics of both the Beijing and Shanghai groups sometimes show up inside the same compromised company, the Beijinggroup tends to focus more on activists, including those involved with Tibetan issues, Stewart said.

He has cataloged about 275 families of malicious software to date.

# Chinese hackers take over fake water utility

## Source: http://www.itnews.com.au/News/352238,chinese-hackers-take-over-fake-water-utility.aspx

## Chinese hackers thought to be linked to the country's government were caught breaking into a United States water plant — without http://www.defencenet.gr/defence/sites/default/files/styles/in_article/public/GALLERY/XAKER%20KINAS.jpgrealising it was a decoy set up by a security researcher.

The MIT Technology Review said the project by Trend Micro security researcher Kyle Wilhoit shows the attacks, which took place in December last year by means of an infected Word document, represent "the most significant proof" of people actively trying to exploit vulnerabilities in industrial control systems (ICS).

According to Wilhoit who observed the attackers taking over the honeypot, "it was 100 per cent clear that they knew what they were doing."

Known as APT1 or the Comment Crew, Wilhoit believes it is the same group of attackers based in Shanghai with links to the Chinese government that has purloined terabytes of corporate data from at least 141 companies since 2006.

Wilhoit has found that roughly half of the criticial attacks on his honeypots come from China, with Germany, UK, France, Palestine and Japan also making the list.

Overall, sixteen countries were involved in the attacks.

Between March and June this year Wilhoit's 12 honeypots attracted 74 attacks, 10 of which took complete control over the dummy ICS.

The findings were presented at the at the annual Black Hat security conference in Las Vegas over the weekend.

Attacks on networked and Internet connected industrial control systems are said to have become more commonplace in recent years.

Earlier this year, the United States Department of Homeland security released a report saying 198 attacks on infrastructure facilities were documented in 2012, many of which were classified as serious.

Most of the attacks in the US were on energy utilities, followed by water companies.

There are now calls for engineers to receive formal training in protecting against infrastructure attacks.

Queensland University of Technology researchers put forward a proposed Australian industrial control systems security curriculum at the 2013 46th Hawaii international conference on system sciences, saying " successful cyber attack has the ability to disrupt and even damage critical infrastructure."

The supervisory control and data acquisition (SCADA) security curriculum aims to provide greater awareness of infrastructure threats, and a five-day vulnerability analysis and system audit course.

Penetration testing and forensic analysis and incident response would also be part of the SCADA security curriculum with full lab facilities available under the proposal.

# Cyber war has arrived in New Zealand

Source: http://i-hls.com/2013/08/cyber-war-has-arrived-to-new-zealand/

The New Zealand Defense Force wants to spend $469 million creating itself a new CYBER army. The kiwis have cut back on their defense force dramatically and this represents a huge investment from a nation which was once defended by six Skyhawks.

Under the plan, the new Network Enabled Army initiative would see combat units kitted out with drones and robots as well as sensors that would monitor the location, the health and condition of soldiers and vehicles.

The Defense Force has invited technology suppliers to a briefing day at its Trentham military base and hopes to take a business proposal case to the cabinet in October.

According to the Sydney Morning Herald program manager Colonel Phil Collett said the spending would be over 20 years and the Defense Force would only be playing catchup with other nations.

**Most of the focus is on drones and robots.** At the moment, the kiwis have no surveillance or reconnaissance systems and it is getting worried at the risk of “friendly fire”. We guess that is because they tend to work closely with the US army. The spending will also involve updating the army’s radios.

Although New Zealand is hoping to award the contract to local developers it is unlikely that they would be able to get it on their own – there are just so many robots which can go into combat strung together with spit and number eight fencing wire.

## U.S. power plants, utilities face growing cyber vulnerability

Source: http://www.homelandsecuritynewswire.com/dr20130819-u-s-power-plants-utilities-face-growing-cyber-vulnerability

American power plants and utility companies face a growing cyber vulnerability. No U.S power plant has so far suffered a significant cyberattack, but experts say preventative actions must be taken to ensure safety.

Utilities provide services which, if disrupted for long periods of time, may result in economic chaos and may even lead to social unrest. Consider the 2003 blackout, which left about fifty million people across North America without electricity for about four hours. That outage, caused by a sagging power line coming in contact with overgrown trees, cost $6 billion.

A cyberattack with intentions to create chaos could inflict far greater economic damage, and cost lives.

Electric Light *&* Power reports that a 2011 report from McAfee and the Center for Strategy and International Studies (CSIS) in Washington, D.C., states that small-scale attacks occur often. According to the report, 85 percent of executives in the power, oil and gas, and water sectors experience network infiltrations, and 25 percent reported they had been victims of a network-related extortion.

Power and utility firms are implementing solutions to prevent and thwart cyberattacks, but security professionals who design cybersecurity systems face several challenges. Utilities are complex systems depending on a variety of instruments and technologies. No pre-package solution or off-the shelf product can fully secure a utility or solve its cybersecurity needs. Security professionals must thus implement customized solutions which are unique to each utility’s systems. These solutions must protect established technology platforms yet remain flexible to adapt to new devices and technologies. Utilities must also consider cyberattacks as both external and internal concerns. Security solutions must therefore protect against staff mishandling of technologies, from downloading software to using file-sharing programs which can expose utility operations to malware and viruses.

Writing in *ELP*, Jose Granado andJosh Axelrod — principal and security practice leader, and senior manager and power and utilities information security sector, respectively, at Ernst & Young LLP —  suggest that when power and utility companies develop a cybersecurity solution,   they should consider the following questions to help identify the risk profile of a facility:

* How does the organization define cybersecurity risk? Does the potential risk affect the business?
* What are the avenues by which such threats might enter the organization’s environment?
* How prevalent are the risks in the industry in which the organization operates? What have the organization’s peers and competitors faced, and what can the organization learn from those incidents?
* What threats might be invited by the behavior of the organization’s own employees? Are the organization’s policies about network access clear and effectively communicated?
* How can the organization align its responses to cybersecurity risk with industry standard security principles, such as ISO 27001/27002 or NIST SP800-53?

After making the determinations, the organization should develop a cybersecurity strategy. Steps utilities should consider include:

* Align cybersecurity to the organization’s overall IT strategy based on the defined risk profile. This helps build support from company board members and top executives, as well as field managers and other personnel.
* Analyze the cybersecurity issues unique to operations, supply, procurement, human resources management, etc., and noting areas of difference and integration.
* Get all parts of the organization working together.
* Rather than focus on tactics to address possible security breaches, develop a cybersecurity approach based on a broad security principle — a rating of breach tolerance, for instance — that can be achieved via several techniques.
* Not assume that a large-scale solution, equivalent to a brand-new IT security system, is needed. Additional security controls implemented for your specific technology environment might be as effective.
* Define the governance and support structure necessary to maintain the solution.

Regulatory and cost concerns cannot be ignored when developing a cybersecurity system. Utilities and power companies face high cost when investing in cybersecurity solutions, and state regulators have not been willing to approve rate hikes to help utilities cover the cost of these investments. Utilities and power companies must not allow lack of government funding or lack of rate increases to undermine security investments, because the cost of not investing in cybersecurity are far too great.