Issue 51, 2013

CBRNE NEWSLETTERRORISM

E-Journal for CBRNE-CT First Responders

CYBER NEWS

Humanity defeated ...

Does it matter who released them?

www.cbrne-terrorism-newsletter.com

ZMap

Source: https://zmap.io/

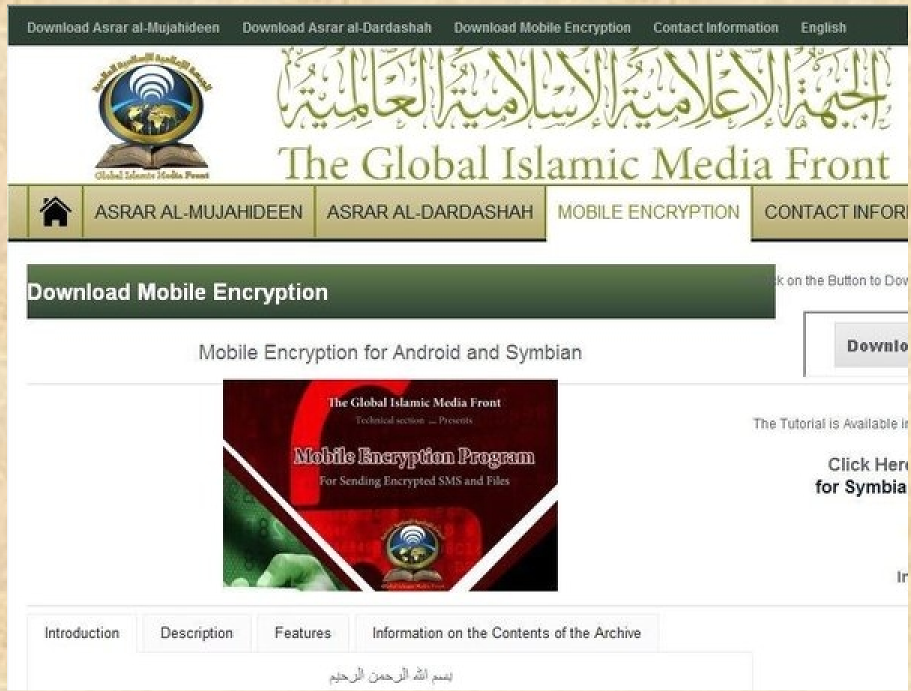
ZMap is an open-source network scanner that enables researchers to easily perform Internet-wide network studies. With a single machine and a well provisioned network uplink, ZMap is capable of performing a complete scan of the IPv4 address space in under 45 minutes, approaching the theoretical limit of gigabit Ethernet.

ZMap can be used to study protocol adoption over time, monitor service availability, and help us better understand large systems distributed across the Internet.

Terrorists, jihadists get new mobile phone encryption software

By Gil Aegerter (Staff Writer, NBC News)

Source: http://investigations.nbcnews.com/_news/2013/09/04/20329081-terrorists-jihadists-get-new-mobile-phone-encryption-software?lite


Download Asrar al-Mujahideen
Download Asrar al-Dardashah
Download Mobile Encryption
Contact Information
English
الجبهة الإعلامية الإسلامية العالمية
The Global Islamic Media Front
ASRAR AL-MUJAHIDEEN
ASRAR AL-DARDASHAH
MOBILE ENCRYPTION
CONTACT INFOR
Download Mobile Encryption
k on the Button to Dow
Downlo
Mobile Encryption for Android and Symbian
The Global Islamic Media Front
Technical section ... Presents
Mobile Encryption Program
For Sending Encrypted SMS and Files
The Tutorial is Available i
Click Here
for Symbia
Introduction
Description
Features
Information on the Contents of the Archive
بسم الله الرحمن الرحيم

New mobile encryption software meant to give jihadists an edge over Western intelligence agencies has been released by an Islamist group that produces propaganda for terrorist groups like al Qaeda, Pakistan's Taliban and Somalia's al-Shabaab.

The Global Islamic Media Front said Tuesday that it had released its "Mobile Encryption Program" for messages and files on mobile phones running the Android and Symbian operating systems. According to the group, the software can encrypt text messages and files and send them via mobile email, even between cell phones with different operating systems. The software also lets users securely check email and prevents users from receiving non-encrypted messages, the group claimed.

The software release was first noted by Flashpoint Partners, a consulting group focused on intelligence and cyber threats.

The front has long offered jihadists a general encryption program and earlier this year released a texting version called "Asrar al-Dardashah," or "Secrets of the Chat."

On its website, the front claims that the new software for direct encryption of material sent to and received from mobile phones "will be a blessing, relief and a secure weapon for our brothers for continuous communication far from the eyes and monitoring of the enemies."

But the efficacy of its previous software releases is unclear, with some calling it simply a rebranding of popular encryption software, and others saying it could be more effective if done well.

"There is no doubt that GIMF produces the premiere proprietary encryption software for jihadists -- in the realm of both Internet messaging and now telephony," Flashpoint senior partner Evan Kohlmann, an NBC News terrorism analyst, said in an email. "There is also no doubt that Al-Qaida has placed its reliance on this technology. AQAP in Yemen, for instance, has encouraged would-be recruits living in western countries to send them ideas for proposed terrorist plots encrypted with GIMF-produced software. We don't really know how effective the encryption is or isn't, because nobody at an official level has publicly disclosed that. However, based on our research, it is likely that U.S. intelligence agencies do have the capability to break that encryption when needed."

Word of the release comes in the wake of news stories detailing the extent of controversial U.S. government technology initiatives aimed at thwarting terrorist plots.

After National Security Agency contractor Edward Snowden released key details of two huge U.S. spying programs this spring, it was reported that terrorists had begun changing how they communicated to evade the NSA.

And last month, a security alert resulted in the closure of U.S. embassies in the Mideast and elsewhere. U.S. officials said the closures came after intelligence services intercepted information that al Qaeda or its affiliates might be planning a large terrorist attack near the end of Muslim holy month of Ramadan. U.S. officials said that the warning was based on a "significant increase in chatter from a growing number of intercepts" in the Mideast. Ramadan ended without an attack.

*NBC News investigative reporter **Robert Windrem** contributed to this report.*

Cybercrime cost Canadians nearly $3.1 billion over past year

Source: http://www.terrorismwatch.org/2013/10/cybercrime-cost-canadians-nearly-31.html

Cybercrime directly cost Canadians $3.09 billion over the past year, according to the newly released 2013 Norton Report.

That jaw-dropping figure reflects the 42 per cent of online adults who were victims of online malfeasance (ie: malicious software, phishing, identity theft, etc.) during the 12-month period ending Aug. 1, and the average cost of cybercrime per individual, which rose 127 per cent, to $383, from the year prior.

While previous reports focused on lack of security, the prevailing issue appears to be lack of common sense.

"Half the people surveyed sleep within arm's reach of their phone. It's become such an extension of what (Canadians) do every day that mindfulness of security is really being limited," said Lynn Hargrove, director of consumer solutions at Symantec Canada, the parent company of Norton.

Risky social media behaviours, use of public or unsecured WiFi, and poor mobile security IQ are all cited as factors.

The 13,022-person survey suggests that 32 per cent of Canadian smartphone users, and 38 per cent of those worldwide, experienced mobile cybercrime over the past year. A further 60 per cent of Canadian mobile device owners, versus 57 per cent worldwide, said they weren't aware that security solutions for such gadgets existed.

Forty-two per cent of Canadians don't log off after each social media session, while 28 per cent share their social media passwords with others. And when it comes to public or unsecured WiFi, fully 60 per cent of respondents said they use it (50 per cent access email over such a connection, 51 per cent use it to access social media sites, 21 per cent to shop online, and — perhaps most shockingly — 24 per cent to do online banking).

"Everyone wants the ability to be connected anywhere, anytime, but it comes with a risk," said Hargrove, noting that the consequences can entail "anything from obvious financial losses, like money out of your credit card or bank account, to lost dollars of work, to the cost of getting your information back."

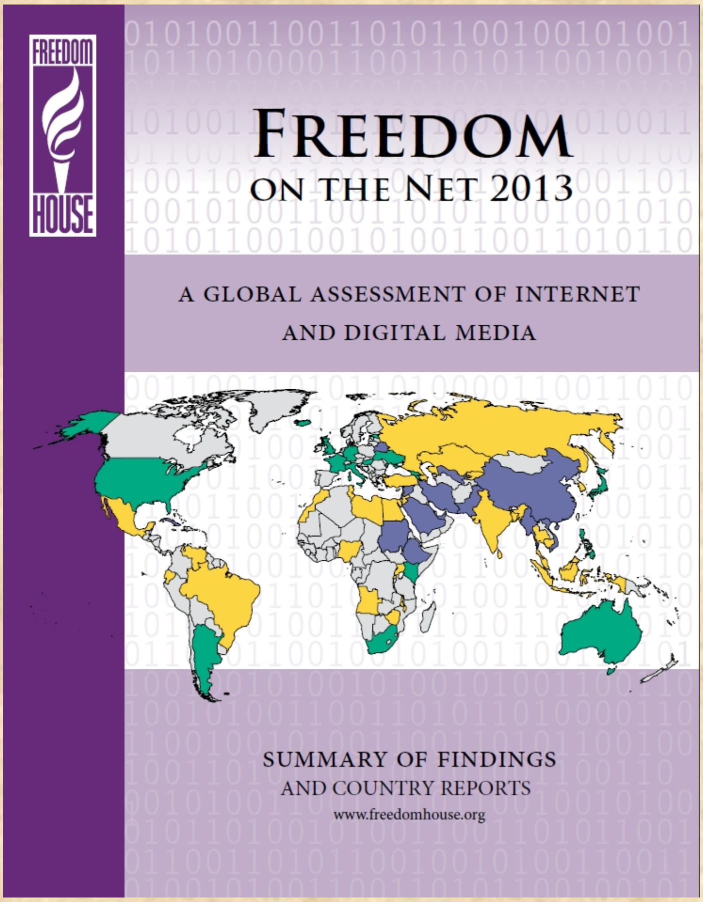
The 24-country survey was conducted online with adults age 18 to 64 between July 4 and Aug. 1. The global results are considered accurate within 0.9 percentage points, 19 times out of 20, while the Canadian data — which draws on 500 respondents — yields a margin of error of 4.4 percentage points.

Pakistan named 'least free' country in world on Internet freedom: Report

Source: http://zeenews.india.com/news/net-news/pakistan-named-least-free-country-in-world-on-internet-freedom-report_881026.html

A report on the level of internet and digital media freedom in 60 countries has revealed that Pakistan is among the bottom ten countries of the list for being 'least free'.

The Freedom on the Net 2013 report, in which the countries are ranked from 0 (the most free) to 100 (the least free), has scored Pakistan 67 and a status of 'not free', while Iceland was at the top with a score of 6.


FREEDOM HOUSE
FREEDOM ON THE NET 2013
A GLOBAL ASSESSMENT OF INTERNET AND DIGITAL MEDIA
SUMMARY OF FINDINGS AND COUNTRY REPORTS
www.freedomhouse.org

It was researched and compiled by Digital Rights Foundation, Pakistan along with research analysts of independent watchdog Freedom House.

Digital Rights Foundation Executive Director, Nighat Dad said that Pakistan remains one of the worst countries when it comes to online freedom of speech, user rights and citizens' privacy.

He further added that the state has been rigorously trying to implement the best of surveillance set-ups to create a kind of watchdog upon activists, journalists and a common citizen on the name of war against terrorism, Express Tribune reports.

The report suggests that despite the growing number of internet users in the country, there have been various political and social obstacles by successive governments that came into power, in the name of fighting terrorism and preserving Islam.

Only urban cities such as Karachi, Lahore, Islamabad and Peshawar have access to better quality broadband services, however, 'bureaucratic hurdles' are causing a problem for the development of 3G or 4G networks in the country.

The list places neighboring India in the 'partly free category' with a score of 47, while China and Iran score even lower than Pakistan with scores of 86 and 91 respectively.

▶**You can read full report at:**
http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf

Cyber Survival: Why We're Losing and What's Needed to Win

By Steven Chabinsky

Source: http:// www.acdemocracy.org

Cyber security is not just about the computer on your desk, or even the remote computer sitting somewhere in what we now call the cloud. A different way of looking at it is to consider cyber security an issue that concerns any technology that has a computer chip in it. Cyber security issues extend to information and information systems, and increasingly they extend to products and services we use in our day-to-day lives. We are facing a technology issue in which similar vulnerabilities exist to your information as they do, for example, to the new generation of biomedical implant devices that allow for remote diagnostics.

When we think about the harms that can befall our information, information systems, products and services, we typically categorize them into categories involving risk to their confidentiality, integrity, and availability. Every day in the newspapers we read about harms to confidentiality. Everyday someone's online data is compromised and corporate trade secrets stolen. But, that's not what keeps most people up at night.

Rather, the possibility of having integrity problems, where you cannot trust the data that you're seeing, is a far greater problem. The idea that you could alter perceptions through technology is the digital equivalent of the Mission Impossible movie where a security camera is in the corner of a room, but the night watchman is deceived by the spy who created a picture of the room empty, put it at the right focal length in front of the camera, and then went on to do anything in the room he wanted.

The cyber equivalent is happening now. Indeed, it happened ten years ago to the electric power grid, when software failures in an Ohio operations center resulted in computer screens that never updated to reflect the developing, and increasingly bleak, situation. As far as the control room was concerned, everything was great. Meanwhile, there was a rolling blackout and the Midwest witnessed the shutdown of over 250 power plants that included 10 nuclear power stations. So, you might be inclined to say, "but that wasn't from a hacker, I remember it was merely a computer glitch." You would be right. Still, I'm reminded of the saying that anything that can happen by accident can happen on purpose. In other words, just because this particular example was accidental, don't feel a false sense of hope that the next time it won't be intentional and calculated to result in maximum harm.

In addition to crimes against confidentiality and integrity, we are concerned with issues of availability. Talks about availability tend to focus on Distributed Denial of Service, or DDoS, attacks, the idea that somebody is sending so much traffic to a website or server that nobody can access it. Worse yet, though, you might have seen what happened last year to Saudi Aramco, the most valuable company in the world, which reportedly fell victim to a malware infection that purposefully destroyed 30,000 of their computers. Yes, thirty thousand.

As you can see, cyber security concerns extend beyond someone viewing your personal information. The big-ticket items involve information and technology that is rendered unreliable, untrusted, and left irreplaceably in ruins. As to these issues, Bill Forstchen's novel, One *Second After* must be considered one of the most significant works of our time. In it, we are exposed to the nightmares of what happens when technology is no longer available to us. One of the most remarkable aspects of the novel in my view, the core of its brilliance, is that it is set in a small town, an area that is rural and not densely populated, where you would consider it most likely that people can survive without technology. Yet, even there we find utter chaos, confusion, and death. You can only extrapolate from that small town to imagine what is happening in the major cities.

And so, when I hear people talk about a cyber 9/11, or a cyber Pearl Harbor, I'm quite dismissive of those as being appropriate analogies. Instead, what I believe is that we very much might face the equivalent of a cyber Katrina. Where we don't have resources, we don't have potable water, we don't have electricity. What we have are all of the cascading harms that are reflected in Bill Fortschen's writings, which are every bit or more as devastating as planes with bombs or planes as bombs. These effects are real possibilities, and nations recognize it. Only a couple of years ago, the China Youth Daily featured an article expressing, "Just as nuclear warfare was the strategic war of the industrial era, cyber-warfare has become the strategic war of the information era, and this has become a form of battle that is massively destructive and concerns the life and death of nations."

Non-nuclear electromagnetic pulse is certainly an emerging threat against availability and, as a result, an emerging risk to our very way of life. I greatly appreciate the efforts of the American Center for Democracy in bringing thought leadership and emphasis to this important topic. Of more immediate concern, however, may be EMP's baby brother, "purposeful interference," more commonly known as jamming. We already are seeing people with $25 illegal jammers interfere with the electromagnetic spectrum, most commonly focused on impeding mobile communications. Think about a situation that requires emergency responders to talk with each other, perhaps an active shooter scenario, hindered through purposeful interference.

We are only now beginning to understand how reliant we have become on wireless devices. But, it's not just about your phone calls, although it certainly includes those. It's not just about being able to check your email, although it includes that as well. In addition, it may be about critical infrastructure and the ability, for example, to change train tracks through wireless communications. And then we have GPS. When people think about GPS they immediately think about positioning and navigation. But an additional feature of GPS that we've grown increasingly reliant upon is its timing signal. And so, if you could interfere with GPS, the timing elements that we've relied upon for interoperability and synchronization of networked systems could be rendered inadequate, if not entirely useless.

Stepping back for a moment, we are forced to take in the entire picture of how vulnerable all of our data and systems are, how they can impact our critical infrastructure, our privacy, and even our personal health. On top of that, we must consider the world economy. Everybody knows that our economy no longer runs on a gold standard. There's no precious metal that reflects every dollar we have. However, what most people don't stop to consider is that there is no physical dollar that represents every dollar we have. At the end of the day, these are mostly accounting entries that get rationalized in the trillions of dollars, and the integrity of that data is what makes up the world's economy.

Yet, despite our increasing reliance upon data integrity and security, our culture has created a demand for products and services that are quick to market without resilience, or reliability, or secondary systems in place should our new, untested ways fail. This is quite serious, and I appreciate the opportunity to discuss this with everyone here in order to focus our mutual efforts on improved security.

[Rachel Ehrenfeld: What do you think can be done?]

I think that there are solution sets. One thing, I believe, is that we have failed in a meaningful way to exercise common enterprise risk management principles in this area. We tend to treat the entire Internet and our technologies as needing to share a common environment. It is almost as though we think everyone needs the same levels of privacy and security, and as a result that everyone should use the same Internet protocols and standards for interoperability. This is quite preposterous. When I go to the gas station, I can't use a diesel pump to put gas in my regular car. The nozzle simply won't fit. But when I was working at the FBI, I had an unclassified computer, a secret computer, and a top-secret computer, and I could use the same thumb drive to move data back and forth between all of them (although I didn't). The computers were differentiated only by the stickers we put on them, indicating their classification levels. The computers themselves were the same computers that are available to you in any common consumer store. So that's the first thing. That has to change. We've got to figure out that there are different priorities and that our security posture needs to be different depending on those priorities.

The second thing is, you cannot have meaningful security without meaningful threat deterrence unless we all decide to live in a bunker. It's just not a possibility. When you think through the risk model, you only have three levers to work from. You could lower the threat, you can lower the vulnerability, or you can lower the consequences. That's what you get to play with; those are your opportunities. We have seen the almost tunnel-like focus on vulnerability mitigation over the past 15 years. It is impossible to create software and hardware that is interoperable, impenetrable, and iterative. That is as absurd, or actually more absurd, than thinking of creating physical environments where communities are impervious to intentional attack. It is not in any way, shape, or form a possibility. It is even worse, I would postulate, in the technology area because it's less static than a building. Technology is dynamic; it is constantly evolving with new software, new hardware, and new applications, with each one being quicker to market than the earlier version.

What you see as a result of this is that vulnerability mitigation has worked best in the area of reducing cyber crimes of opportunity, and even then it has serious limitations. We patch our systems, we update our software, and as a result the common criminal doesn't break into those better-protected systems. They break into the systems that haven't done that. That's the same as in the real world. If someone just wants a TV, and your house has the door locked, they don't go to your house; they go to the one that doesn't have the door locked. Now, query for a second if everybody locked their doors what would happen? You would see a shift. Burglars would start going through windows, and vulnerability mitigation practices would repeat themselves in that context. In essence, best practices would be raised to protect doors *and* windows.

Obviously there's a point where vulnerability mitigation efforts need to stop. We don't start first with locks on doors, then with locks on doors and windows, then with bars on doors and windows, and then with underground bunkers. That's not how it works. Instead, we immediately shift to threat deterrence once standard vulnerability mitigation opportunities are no longer cost effective. We put up alarms, we put up video cameras, and those basically say to the adversary: we concede the ground, but now it's no longer about us. It's about you. You can get in, but now we're going to detect you, we're going to find you, and you will suffer a penalty. It won't be worth it for you.

Could you imagine if in your place of business the alarm went off at 3:00 in the morning, and the monitoring company calls you. And they say: someone just broke through the front door of your place of business, but don't be concerned we have the locksmith on the way. How absurd, right? We don't do that. We call the police. And that is the only reason why burglars don't like to rob places that have alarm systems. It's not the noise that bothers them.

Yet, every day, tens of thousands of times a day, across this country we have enemies who are trying to break into our critical infrastructure, into our military institutions, and the response has been to tell the chief information security officer: Make sure you're continuously monitoring to patch your systems. It doesn't work, it won't work, it will never work.

So the next strategic opportunity is after we figure out what's important, to make sure that we build the software, hardware, and protocols necessary for detection, attribution, and penalty based deterrence.

There are opportunities here that, I think, actually are a happy coincidence. I would suggest that in a lot of areas where security is the most needed, privacy rights are actually not the most necessary. Take the electric power grid, for example. The electric power grid is a high security system in which the owners and operators do not want or need anonymity. No one who isn't authorized should be touching those systems. The owners, operators, and employees of an electric power company want perfect attribution. So that's an area that's ripe for new software, new hardware, new security policies, and less interoperability, all of which should add up to say to would-be attackers: if you are found in our infrastructure (and you will be, because we have designed this system for detection and attribution), there will be penalties.

So, I think there are opportunities, but the first step is to distinguish what we need to protect most, to build in proper threat deterrent models that promote detection and attribution consistent with privacy demands, and then to ensure that policies and resources are in place that will make the possibility of our adversaries being brought to justice a reality.

***Steven Chabinsky** is former Deputy Assistant Director, FBI Cyber Division; Senior Vice President of Legal Affairs and Chief Risk Officer, CrowdStrike.*

Police warning after drug traffickers' cyber-attack

Source: http://www.bbc.co.uk/news/world-europe-24539417

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

Drug traffickers recruited hackers to breach IT systems that controlled the movement and location of containers.

Police carried out a series of raids in Belgium and Holland earlier this year, seizing computer-hacking equipment as well as large quantities of cocaine and heroin, guns and a suitcase full of cash.

Fifteen people are currently awaiting trial in the two countries.

Mr Wainwright says the alleged plot demonstrates how the internet is being used as a "freelance marketplace" in which drug trafficking groups recruit hackers to help them carry out cyber-attacks "to order".

"[The case] is an example of how organised crime is becoming more enterprising, especially online," he says.

A Europol official tells Tom Bateman how traffickers hacked into the IT system at Antwerp port

"We have effectively a service-orientated industry where organised crime groups are paying for specialist hacking skills that they can acquire online," he adds.

Vanishing containers

The attack on the port of Antwerp is thought to have taken place over a two-year period from June 2011.

Prosecutors say a Dutch-based trafficking group hid cocaine and heroin among legitimate cargoes, including timber and bananas shipped in containers from South America.

The organised crime group allegedly used hackers based in Belgium to infiltrate computer networks in at least two companies operating in the port of Antwerp.

The breach allowed hackers to access secure data giving them the location and security details of containers, meaning the traffickers could send in lorry drivers to steal the cargo before the legitimate owner arrived.

Workers were first alerted to the plot when entire containers began to disappear from the port without explanation.

"These criminal organisations always look for a new way to get drugs out of the harbour," says Danny Decraene who heads the Antwerp organised crime unit of the Belgian Federal Police.

"In this case they hired hackers [who were] very high level, intelligent guys, doing a lot of software work," he adds.

He says the operation to hack the port companies took place in a number of phases, starting with malicious software being emailed to staff, allowing the organised crime group to access data remotely.

When the initial breach was discovered and a firewall installed to prevent further attacks, hackers broke into the premises and fitted key-logging devices onto computers.

This allowed them to gain wireless access to keystrokes typed by staff as well as screen grabs from their monitors.

Assault rifle attack

Mr Decraene says the total quantity of drugs trafficked by the group is unknown, but in a series of raids earlier this year police seized more than a tonne of cocaine, with a street value of £130m, and a similar amount of heroin.

In January a lorry driver unconnected to the plot was shot at after he had unwittingly driven a container allegedly filled with cocaine from the terminal at Antwerp.

The attack took place in the province of Limburg, where suspects armed with AK-47 assault rifles fired at the driver, who was unharmed.

Following the cyber-attack in Antwerp, a joint operation by Belgian and Dutch police resulted in raids on more than 20 homes and businesses.

Officers seized six firearms including a machine gun and silencer, bullet-proof vests, and 1.3m euros (£1.1m) in cash inside a suitcase.

Mr Wainwright says the IT attack is consistent with a "new business model" of organised crime activity and he says he expects this kind of cyber-security breach to "become a more significant feature in future" of drug trafficking.

"What it means therefore is that the police need to change the way they operate - they have to become much more tech savvy," he says.

"But also I think governments and parliaments need to help us to make sure therefore that we have the right laws to fight back against this massive exploitation of the internet," he adds.

Container companies operating out of the port of Antwerp say their IT security has now been improved.

Weekend Attacks on Arkansas' Electric Grid Leave 10,000 Without Power

Source:http://www.nationalterroralert.com/2013/10/08/weekend-attacks-on-arkansas-electric-grid-leave-10000-without-power-you-should-have-expected-u-s/?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+NationalTerrorAlertResourceCenter+%28National+Terror+Alert+Response+Center%29&utm_content=Yahoo!+Mail

More than 10,000 people in Arkansas were dumped into a blackout Sunday following an attack on that state's electric grid, the FBI said today, the third such attack in recent weeks.

The FBI said that two power poles had been intentionally cut in Lonoke County on Sunday, resulting in the outage.

The FBI said it would pay a $25,000 reward for information about the attacks.

And for good reason. The FBI suspects these attacks are linked with a third incident in September.

According to the FBI:

In the early morning hours of September 29, 2013, officials with Entergy Arkansas reported a fire at its Keo substation located on Arkansas Highway 165 between Scott and England in Lonoke County. Fortunately, there were no injuries and no reported power outages. Investigation has determined that the fire, which consumed the control house at the substation, was intentionally set. The person or persons responsible for this incident inscribed a message on a metal control panel outside the substation which reads, "YOU SHOULD HAVE EXPECTED US"

John McAfee predicts hackers will empty Obamacare enrollees' bank accounts

Source: http://washingtonexaminer.com/john-mcafee-predicts-hackers-will-empty-obamacare-enrollees-bank-accounts/article/2537153

Obamacare websites have "no safeguards" to protect Americans who enroll in the health insurance exchanges from hackers who will "empty your bank account," according to internet security pioneer John McAfee.

INSURANCE EXCHANGES
OCTOBER 6: HHS OFFICIALS ACKNOWLEDGE THAT HEALTHCARE.GOV NEEDED DESIGN CHANGES
FOX FACTS
FOX NEWS
1:45 CT
MCAFEE: EASY FOR FAKE WEBSITES TO POSE AS OBAMACARE WEBSITES
The REAL STORY
TO THE INTL BODY OVERSEEING THE DESTRUCTI
NAS ▲ 27.70
0:00 / 3:39

McAfee said he could create a fake Obamacare exchange website for "a couple hundred dollars" and expect a big return on the scam.

"I'll ask you your social security, your date of birth, [so] an hour later I can empty your bank account," he told Fox News' Gretchen Carlson.

"And this is going to happen, it's going to happen soon. Nothing in the Obamacare system safeguards against this," he said.

The interview was a follow-up to McAfee's conversation with Fox's Neil Cavuto last week.

"There is no central place where I can go and say, 'OK, here are all the legitimate brokers and examiners, for all of the states,' and pick and choose one," McAfee told Cavuto.

"[I]nstead, any hacker can put a website up, and make it look extremely competitive, and because of the nature of the system — this is health care, after all — they can ask you the most intimate questions and you're freely going to answer them."

Physicians feared terrorists might hack Dick Cheney's cardiac defibrillator

Source: http://www.homelandsecuritynewswire.com/dr20131021-physicians-feared-terrorists-might-hack-dick-cheney-s-cardiac-defibrillator

In a 60 Minutes segment aired yesterday (Sunday), former vice-president Dick Cheney told the interviewer that his doctors turned off the wireless function of his implanted cardiac defibrillator (ICD) "in case a terrorist tried to send his heart a fatal shock." The *Washington Post* reports that,

Years later, Cheney watched an episode of the Showtime series "Homeland" in which such a scenario was part of the plot.

"I found it credible," Cheney tells "60 Minutes" in a segment to be aired Sunday. "I know from the experience we had, and the necessity for adjusting my own device, that it was an accurate portrayal of what was possible."

Forbes asked three experienced electrophysiologists — these are the cardiologists who implant ICDs – whether this the 60 Minutes segment described a realistic scenario. The three doctors said that as far as they knew, this has never happened in the real world but that it is impossible to rule out the possibility.

Here is the answer given by one of the doctors, Westby Fisher, who practices at NorthShore University HealthSystem in Evanston, Illinois, and is a Clinical Associate Professor of Medicine at the University of Chicago's Pritzker School of Medicine:

> Daniel Halperin with William Maisel, MD and colleagues set out to hack a Medtronic ICD and did in a paper published in 2008 in IEEE.

They were within 4 inches of the device and reverse-engineered the telemetry protocol. Their point: data are not encoded. This since has been changed, but devices that once used electromagnetic coupling have been "upgraded" to radio waves in the medical frequency (400-405 MHz). Though no device has ever been hacked with the new technology to my knowledge, the new technology offers potential opportunities IF an electromagnetic handshake first weren't required, like it is now.

Cheney's paranoia was a bit excessive, but then again, who knows in the world of espionage…

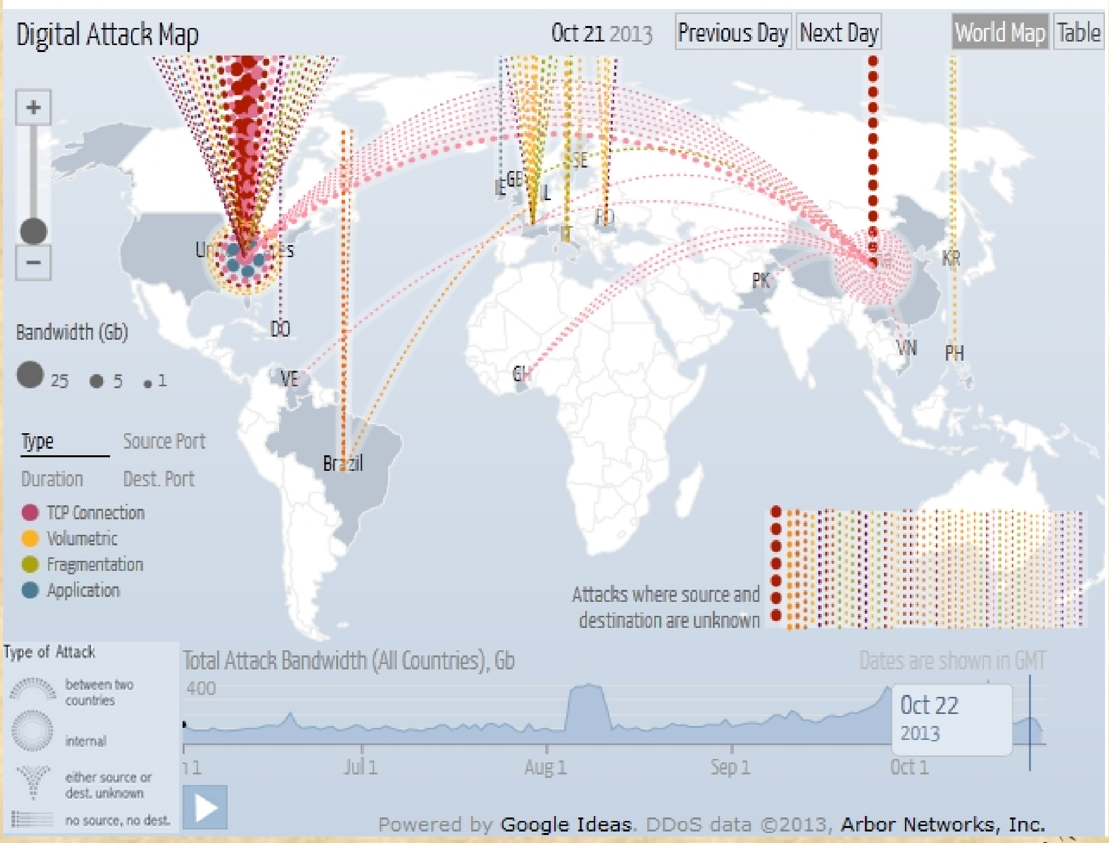
Edward J Schloss, the medical director of Cardiac Electrophysiology at the Christ Hospital in Cincinnati, Ohio, told *Forbes*: "If I were the vice president, I would probably want to work with industry to minimize my risk."

— Read morein Daniel Halperin et al., "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," IEEE Symposium on Security and Privacy *(2008): 129-42*

Google's Digital Attack Map plots DDoS attacks around the world

Source: http://grahamcluley.com/2013/10/google-ddos/?goback=.gde_4709642_member_5798733833410994179#!

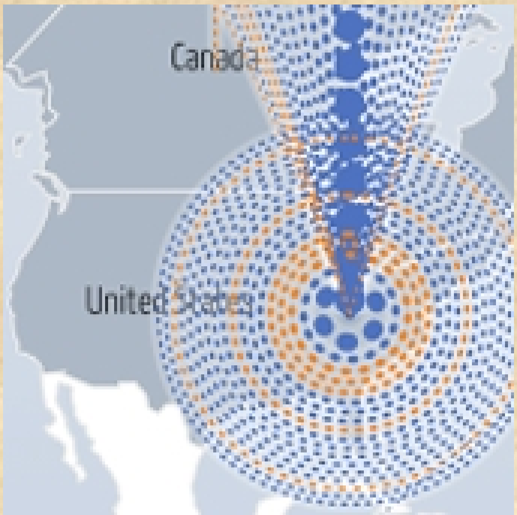
One of the most common attacks seen against a website is a distributed denial-of-service (DDoS) attack, where malicious hackers command botnets of hijacked computers around the world to bombard a particular website with traffic – causing it to fall over.



The team at Google Ideas has teamed up with Arbor Networks to provide Digital Attack Map, a visualisation of denial-of-service attacks around the world.

There's even a movable timeline, so you can look back through at historic attacks (see the enormous DDoS attack which started on August 8 2013, for instance, when the United States was getting pounded).

The threat of DDoS attacks have been used by hackers in the past to blackmail websites into paying "protection money", or risk having their site go offline. Victims have included gambling sites in the run-up to major sporting events.



However, in recent years it has become a favourite weapon of hacktivists and politically-motivated attackers who wish to silence a website that they dislike.

Of course, it's not just the owners of the websites themselves who are the victims in this kind of online bombardment. Regular computer users suffer too – both by not being able to visit particular sites, but also by having their own computer participating in the attack.

Obviously, the best thing is to avoid having your computer recruited into a botnet in the first place.

You can reduce the chances of that happening by keeping your anti-virus software up-to-date, deploy a layered defence in your company rather than just relying on one technology, and install the latest security patches for your operating system and programs such as Adobe Flash, PDF Reader, and Java.

Remember – if your computer has been recruited into a botnet, it might not just be launching DDoS attacks. Hackers could just as easily steal your files, read your email, spy on every keypress you make, launch spam and malware campaigns, and even watch you through your webcam.

If Google's Digital Attack Map raises the public's awareness of the DDoS and botnet risk, then it will have been a job well done.

Terrorism insurance should cover cyberterrorism: industry

Source: http://www.homelandsecuritynewswire.com/dr20131024-terrorism-insurance-should-cover-cyberterrorism-industry

The Terrorism Risk Insurance Act (TRIA) is a federal backstop designed to protect insurers in the event an act of terrorism results in losses above $100 million. Industry officials question whether cyber terrorism is covered by the program, which is administered by the Treasury Department.

Molly Lang and John Mullen write in the *Insurance Journal* that the reality of cyberthreats which might cause damage exceeding $100 million, and the relationship of such damages to TRIA, should be discussed as the reauthorization of TRIA nears. The program was established in 2002, and has been reauthorized twice, most recently by the Terrorism Risk Insurance Program Reauthorization Extension Act of 2007.

TRIA is scheduled to expire on 17 December 2014, and the need to consider cyber threats in the reauthorization of the program was reinforced by former Secretary of Homeland Security Janet Napolitano in her farewell address. She said that the United States will "at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society."

For the purpose of TRIA coverage, an act of terrorism must be certified as such by the Treasury Secretary, in agreement with the Secretary of State and the Attorney General.

Experts say that acts of cyber terrorism could result in losses exceeding $100 million, but the insurance industry questions whether cyberterrorism would be considered, under TRIA, as an act dangerous to human life, property, or infrastructure. The insurance industry is also concerned that the geographic limits placed on TRIA do not accurately address the potential impact of cyber terrorism. The *Insurance Journal* notes that a 2002 insurance industry conference report, for example, suggested that the original version of TRIA was intended to cover cyber terrorism, but primary policy coverage may not cover damages from cyberattacks.

The insurance industry is exploring the relatively new market of cyber liability and many in the industry are pushing for clarification of the application of the TRIA program to cyberterrorism.

The Federal Insurance Office (FIO), tasked with assisting the Treasury Department in administering TRIA, is aware of cyberterrorism risks and their implications for the insurance industry. The FIO, FBI, and Treasury Office of Critical Infrastructure Protection have been studying cyberattacks and their likely effects within the financial sector.

Congress has held hearings on reauthorizing TRIA, and while the act has bipartisan support, there is a debate about whether the program should be modified. The proposed modifications to the act include providing a timeframe for the certification process to changing the deductible, aggregate threshold, and copay percentage. The three TRIA reauthorization bills did not address the issue of cyberterrorism.

“Terrorism risks have evolved since TRIA was enacted and cyber terrorism is a real threat,” Lang and Mullen note. “The Program should not simply be reauthorized with a blanket stamp of approval, but there needs to be discussion about whether acts of cyber terrorism should be explicitly included in TRIA.”