USA under attack? Who is next?

▶ London ▶ Paris ▶ Stockholm ...

CBRNE Newsletter Terrorism

Volume 49, 2013

Cyber News

www.cbrne-terrorism-newsletter.com

Future computers will identify users by thoughts, not passwords

Source: http://www.homelandsecuritynewswire.com/dr20130410-future-computers-will-identify-users-by-thoughts-not-passwords

Instead of typing your password, in the future you may only have to think your password, according to University of California, Berkeley

School of Information (I School) researchers. A new study explores the feasibility of brainwave-based computer authentication as a substitute for passwords.

The project was led by School of Information professor John Chuang, along with Hamilton Nguyen, an undergraduate student in electrical engineering and computer science; Charles Wang, a first-year I School MIMS student; and Benjamin Johnson, formerly a postdoctoral scholar at the I School. Chuang presented the team's findings this week at the 2013 Workshop on Usable Security at the Seventeenth International Conference on Financial Cryptography and Data Security in Okinawa, Japan.

A University of California, Berkeley release reports that since the 1980s, computer scientists have proposed the use of biometrics for computer authentication.

Systems requiring fingerprint scans, retina scans, or facial or voice recognition are far more secure than passwords, since fingerprints are hard to forget and harder to steal. Such systems, however, are also slow, intrusive, and expensive. Biometric authentication has never gained wide acceptance; other than a few high-security settings, it remains more science fiction than science fact.

In recent years, security researchers have proposed using electroencephalograms (EEGs), or brainwave measurements, for computer authentication, replacing passwords with "pass-thoughts." If other biometric systems have proven cumbersome and expensive, however, brainwave authentication has been even more so; no one wants to install invasive probes under their skull every time they check their e-mail!

All that has changed, though, with recent developments in biosensor technologies.

New consumer-grade EEG devices

Traditional clinical EEGs typically employ dense arrays of electrodes to record 32, 64, 128, or 256 channels of EEG data.

New consumer-grade headsets, on the other hand, use just a single dry-contact sensor resting against the

user's forehead, providing a single-channel EEG signal from the brain's left frontal lobe.
The research team used the Neurosky MindSet, which connects to a computer wirelessly using Bluetooth and can be purchased for approximately $100. "Other than the EEG sensor, the headset is indistinguishable from a conventional Bluetooth headset for use with mobile phones, music players, and other computing devices," according to the researchers.

Will it work?

Will this new technology work for computer authentication? Is it secure, accurate, and reproducible enough to replace passwords? More importantly, would people actually be willing to use it? The research project has

preliminary answers to all three of these questions: yes, yes, and (probably) yes.
The release notes that the team conducted a series of experiments to determine whether the single EEG channel provided high enough signal quality for accurate authentication. For authentication, the computer needs to be able to accurately and consistently distinguish your brainwave patterns from someone else's.
By selecting customized tasks for each user and then customizing each user's authentication thresholds, the team was able to reduce error rates to below 1 percent, comparable to the accuracy of more invasive multi-channel EEG signals.
Accuracy is not enough. however. If a system is a pain, people will refuse to use it, no matter how accurate it is. The new generation of brainwave readers are much more user-friendly than before, but the team also focused on finding mental tasks that are enjoyable to users.

Seven mental tasks

The researchers measured participants' brainwaves while they performed seven different mental tasks. Users were asked to do two types of tasks: three where everyone performed the same task and four where users had individual secrets. For tasks of the first group, participants were asked to focus on their own breathing, imagine moving their finger up and down, or listen for an audio tone and then respond to the tone by focusing on a dot on a piece of paper.
In tasks where participants could choose a personalized secret, they were asked to imagine performing a repetitive motion from a sport of their choice (like swinging a golf club or kicking a ball), imagine singing a song of their choice, watch a series of on-screen images and silently count the objects that match a color of their choice, or choose their own thought and focus on that thought for ten seconds.
All seven of the tasks provided enough information to successfully authenticate the users. In fact, the personalized tasks weren't significantly more accurate than the tasks where everyone did the same thing. The key to the success of a brainwave authentication system, then, is finding a mental task that users will not mind repeating on a daily basis. Researchers found that users would prefer to repeat tasks that are fairly easy but not too boring. Users' favorite tasks included counting objects of a specific color, imagining singing a song of their choice, or simply focusing on their own breathing. Several users found it difficult to imagine performing an action from their favorite sport: they found it unnatural to imagine the movement of their muscles without

actually moving them. Similarly, when asked to choose their own "pass-thought," many users chose a thought that was complicated or difficult to repeat. Imagining moving a finger up and down was boring to the majority of participants.


New headsets use a single sensor resting against the forehead. (photo by Cory Doctorow)

Computer systems of the future

The release says that computers that recognize you by your brainwaves might seem like a futuristic fantasy, but these experimental results suggest that that future is more realistic than we might have suspected. "We find that brainwave signals, even those collected using low-cost non-intrusive EEG sensors in everyday settings, can be used to authenticate users with high degrees of accuracy," the researchers conclude.

Rather than being limited to ultra high-end, high-security systems, brainwave-based authentication could end up being as cheap, accessible, and straightforward as thought itself.

Terrorism in Cyberspace: Hezbollah's Internet Network*

Source: **http://www.terrorism-info.org.il/en/article/20488**

1. For **Hezbollah, its cyberspace presence is of great importance, and is considered by both Hezbollah and Iran as an important weapon in the battle for hearts and minds**. Hezbollah and Iran use the Internet for both **internal information and indoctrination** (in Lebanon, the Shi'ites and its own operatives) and **external pro-Iranian propaganda** (especially the Arab-Muslim world and the West). The network enables Hezbollah to circumvent the limitations placed on its other media (television, radio, the press) by the West, especially the United States.
2. Today Hezbollah's vast media network includes a **satellite television channel** (Al-Manar TV), **a radio station** (Radio Nur), **the press** (Al-Ahad/Al-Intiqad) and **network of websites**. Hezbollah also uses the social networks, YouTube and various Lebanese media which it does not own but which are affiliated with it, to publicize its positions and policies (for example, the newspaper Al-Akhbar and the Al-Mayadeen TV channel).
3. During the past decade Hezbollah developed an extensive Internet presence, much larger than those of the other terrorist organizations. Since the Second Lebanon War (2006), and with greater intensity during the past year, **Hezbollah has increased its Internet presence,**

improved its quality and upgraded it technically. Currently (updated to March 2013) Hezbollah has **more than 20 websites in seven languages**, some of them news sites and some of them relating to specific issues. The sites are used by senior Hezbollah figures, the organization's social institutions, its media and several important Shi'ite villages in south Lebanon where Hezbollah is entrenched.

4. From the point of view of a terrorist organization like Hezbollah, developing and maintaining such a broad Internet network in particular and its media empire in general is very expensive. It also necessitates technical capabilities and trained manpower. In our assessment, Iran supports the development and maintenance of **Hezbollah's Internet presence and media empire, which exceed, both in extent and capabilities, Hezbollah's needs in Lebanon per se**. In addition, Iran itself operates two Farsi websites devoted to Hezbollah.

5. **The propaganda and information strategy of Hezbollah's websites is uniform,** and both serves the organization and promotes Iran's ideology and political agenda. In our assessment, **media strategy is formulated by Hassan Nasrallah and the Hezbollah leadership, based on overall Iranian strategy**. Hezbollah's media policy **is coordinated with Iran**, whose policies and considerations are well known to senior Hezbollah figures.

The Main Themes of Hezbollah's Websites

6. **The main themes of Hezbollah's websites are the following**:

1) **Glorifying the organization, representing it as a force gaining in strength while Israel is represented as growing weaker and about to collapse: That includes messages of deterrence for Israel**, which also serve Iranian strategy. Such messages were more conspicuous during the past year, resulting from the open discourse between Israel and Iran regarding the international sanctions imposed on Iran.

Glorifying Hezbollah: Scenes from a 17-part Al-Manar TV documentary entitled "What if Hezbollah were defeated," broadcast beginning December 17, 2012

2) **Fostering the personality cults of Hezbollah leader Hassan Nasrallah and of Hezbollah shaheeds, represented as heroes and role models**. The three principle shaheeds commemorated by the organization are Sheikh Gharb Kharb, Sheikh Abbas Musawi and Imad Mughnieh.

3) **Legitimizing terrorism towards Israel and the West** by cultivating the ideologies of ***shahada*** (death as a martyr for the sake of Allah), ***muqawama*** ("resistance") and **jihad**; at the same time, there is strong condemnation of any Arab or Palestinian peace process and the agreements or arrangements with Israeli they might produce.

4) **The hate industry**: Vicious propaganda and incitement against Israel, the Zionist Movement, the Jewish people, the United States and the West. **Hezbollah rejects the existence of the State of Israel,** calling for its annihilation and the establishment of a Palestinian state on the ruins.

5) **Disseminating Iranian Islamic Shi'ite ideology based on the principles set down by the Ayatollah Khomeini**, including hatred for the United States, the West, Israel and the Jewish people. Hezbollah websites also promote **the**

personality cult of Iranian Supreme Leader Ali Khamenei, representing Hassan Nasrallah as one of his supporters and admirers.

6) **Promoting Hezbollah and Iran's political agenda**: Hezbollah's websites support Iranian policy in the Middle East and its positions concerning the United States and the West. They also foster the "resistance camp," which includes Iran, Syria, Hezbollah and the Palestinian terrorist organizations. During the past year Hezbollah's media, including its websites, were enlisted in **a propaganda campaign to support the Assad regime in Syria** it defaming and criticizing the Syrian opposition and the popular uprising.

Hezbollah's Target Audiences

7. The main **target audience of Hezbollah's websites is Lebanon**, especially the Lebanese Shi'ite population. Hezbollah wants Shi'ite support and to recruit its members as fighters in its ranks. Another **important target audience** is Iran. In our assessment, its second priority is **the Arab-Muslim world**, whose support it also needs. Third in importance are **the West and Israel**, especially their Arab-Muslim communities (exposed to anti-Israeli and anti-Western as well as pro-terrorism incitement through Hezbollah's websites).

The Islamic Resistance in Lebanon website, Hezbollah's leading media website, in Arabic.

The Islamic Resistance in Lebanon website, Hezbollah's leading media website, in English.

8. **Hezbollah's websites appear in seven languages**, the most important of which is Arabic, the language of the Lebanese and Arab target audiences. Until recently, they appeared in **Arabic**, **English**, **French**, **Farsi** and **Hebrew**;[2] **Azeri** and **Spanish** have lately been added. Their addition indicates the importance Iran and Hezbollah give **Azerbaijan and Latin American countries** (in which there are large Arab-Muslim communities, especially Lebanese communities). Thus, through Hezbollah's Internet network, Azeri and Spanish-speaking populations are exposed to anti-West, anti-Israeli and pro-terrorism incitement, with Iranian orientation.

The Popularity of Hezbollah's Websites

9. Despite the efforts Iran and Hezbollah have invested in launching and developing the Hezbollah website network, most of them received **relatively low ratings in a survey conducted of Lebanese news sites**. According to the global web metrics provider Alexa.com, the only Hezbollah website enjoying high ratings the Al-Manar TV website, which in 2012 was rated second of the ten most popular Lebanese news sites (after Tayyar, the site of the Free Patriotic Movement, Hezbollah's opposition in Lebanon. In eighth place was the website of the newspaper **Al-Akhbar**, affiliated with – but not owned by – Hezbollah).

10. Most of Hezbollah's websites, especially those belonging to its social institutions, **are not particularly popular in Lebanon** and especially not beyond its borders. In our assessment that is because **most of its visitors are Shi'ites** (the largest community in Lebanon), **who visit them because of their religious/sectarian slant and because of their clearly Iranian orientation**. On the other hand, most other communities, which are are hostile to Hezbollah

(and its Iranian and Syrian sponsors), prefer websites which do not identify with Hezbollah and Iran's political and ideological agendas.

11. **Hezbollah operates in a number of ways to break through the constraints of its religious-sectarian-political identity**. For example, it makes use of Lebanese media such as **Al-Mayadeen TV** and the newspaper **Al-Akhbar**, which are affiliated with but not owned by Hezbollah. In some instances Hezbollah **tries to blur the identity of some of its websites** and attempts to represent them as **overall-Lebanese or at least generally Shi'ite**. Another marketing tactic is the **large number of languages** used by Hezbollah to appeal to Arab-Muslim communities around the globe, especially those in the West and in Latin America.

Results of a Technical Analysis of Hezbollah Websites[3]

12. Most of Hezbollah's websites receive technical support from Internet companies in **the United States, Europe (Britain, France) and Lebanon**. They provide Hezbollah with IP addresses and/or access to the Internet. In our assessment, most of the time the Internet service providers (ISPs) are **approached by front men or by Internet companies, usually from Beirut,** which not necessarily affiliated with Hezbollah. They are then listed as contact personnel for a number of websites (For further information see below). In addition, as opposed to past practice, **Hezbollah's websites frequently change their IP addresses and ISPs** (almost every year), and each of them has **addresses with various extensions** (.org, .com, .net).

13 In our assessment, using front men and Lebanese Internet intermediaries, like frequently changing ISPs, **has three objectives**: **the first is to blur, insofar as is possible, Hezbollah's ties to the websites** and prevent the ISPs from connecting it to them. **The second is to make if difficult for the authorities in the United States and other Western countries to shut the sites down** (the **United States** is especially problematic for Hezbollah, where Hezbollah is designated as a terrorist organization and where in the past law enforcement authorities used measures against Hezbollah media). **The third** is to prevent cyber attacks. The Palestinian Islamic Jihad, which maintains close relations with Iran, uses similar tactics to make it difficult to identify its websites.[4]

14. Two important websites do not hide their Iranian identities: **Moqawama.ir** is a Farsi site and is registered to the owner of an Internet company in Mashhad, who is head of the culture and communications department of the Islamic information ministry in the province of Razavi Khorasan, in northeastern Iran. The website is devoted in its entirety to Hezbollah and Lebanon. It may be officially or semi-officially run by the Islamic Information Organization in Iran and **promotes Hezbollah's image in Iran**. Another Iranian website is **moqavemat.ir**, **registered to a man living in Iran** (in Qom, and in the past in Mashhad); its IP is with a company in Qom. It mostly posts articles about Iran, combined with relatively scanty coverage of Hezbollah. In our assessment, the website is also operated by Iran to promote Hezbollah's image.

15. **Most of Hezbollah's websites are interactive**: Programs broadcast by its radio station, **Al-Nur**, can be heard on its website; **Al-Manar TV** broadcasts can be viewed, and its newspapers and magazines can be read in PDF format. Moreover, Hezbollah uploads propaganda videos to YouTube, has a Facebook page and a Twitter account, **some of its sites have RSS feeds and others can be downloaded to smart phones**.

16. **The graphic design of Hezbollah's websites has improved in recent years** and there are links to the social networks. In particular, the graphics of the news websites are more professional.

Main Findings of the Analysis of Hezbollah's Websites

17. **Hezbollah websites can be divided into seven general categories according to the functions they serve**:

1) **Category 1 – Main news sites**: Hezbollah's leading news site is **Al-moqawama al-islamiyyah fi-lubnan** ("the Islamic resistance in Lebanon"). It also has other news sites, among them **Moqavemat** ("resistance")**wa-inbaa** ("news") and **Daam al-moqawama al-islamiyya fi-lubnan** ("Support for the Islamic resistance in Lebanon) (which can be accessed through a link in Hezbollah's **Qawem** forum). There was also a now-defunct news site called **Wa'ad** ("promise"). The category also includes the Farsi sites **Moqawama.ir** and **Moqavemat.ir**, which are **apparently run directly by the**

Iranian administration to promote Hezbollah (and Iranian) public relations.

2) **Category 2 – Hezbollah media sites**: Among them are the **Al-Manar TV site**, the **Radio Al-Nur site** and the website of its newspaper **Al-Ahad**, (whose full name is **Al-Ahad/ Al-Intiqad)**.

3) **Category 3 – Hezbollah's social institutions' sites**: Hezbollah's social institutions are active in the fields of health, welfare, education and aid to the needy, particularly from the Shi'ite community. **The institutions are maintained through generous Iranian support, and in several instances they are Lebanese branches of Iranian institutions. They support Hezbollah's military-terrorist infrastructure and are an important platform for spreading revolutionary Iranian Islamic ideology to the local Shi'ite population**. The websites include:

i) **Website of the Martyr's Institute** (Muassasat al-shahid) provides aid to the families of Hezbollah shaheeds.

ii) **Website of the "Construction Jihad"** (Jihad al-binaa) provides social services for the Shi'ite population and deals with initiatives for construction and rehabilitation in south Lebanon.

iii) **Website of the Institute of the Wounded** (Muassasat al-jarha) aids wounded Hezbollah operatives and their families.

iv) **Website of the Islamic Health Authority** (Al-hayaa al-sahiya al-islamiya), an institute providing medical services to Shi'ites and Hezbollah operatives.

v) **Website of the Imam al-Mahdi Scouts** (Kashafat al-imam al-mahdi), Hezbollah's scouting movement, whose goal is to influence the younger generation of Shi'ites and prepare them to join Hezbollah.[5]

vi) **Website of the Imam Mahdi Guides Association** (Jamiat murshidat al-mahdi), a women's association guiding young girls in the spirit of Shi'ite Islam, who participate in social and religious activities affiliated with Hezbollah.

vii) **Website of the Al-Emdad ("aid") Committee**, the Lebanese branch of an Iranian aid society founded by the Ayatollah Khomeini. It helps the needy, including orphans, some of them children of Hezbollah terrorist operatives killed in confrontations with Israel. The society also runs kindergartens, schools and organizations offering vocational training.

viii) **Website of the Islamic Institute for the Study of Culture – the Al-Mahdi schools**, which operates educational institutions used by Iran and Hezbollah to spread Shia and Iranian ideology in Lebanon.

ix) **Website of the Society of Knowledge** (Al-Maaref), an association established in 1996 to spread Khomeini's version of Shi'ite Islamic ideology. It has dozens of cultural and religious centers which operate in the spirit of Khomeini's ideology, and also publishes books and newspapers.

x) **Website of the Friends of the Environment**, an association affiliated with Hezbollah, although it represents itself as Lebanese-nationalistic. It maintains a pretense of being oriented towards ecology, but in fact its activities focus on Hezbollah's propaganda campaign (in collaboration with other Hezbollah-affiliated organizations). The campaign trumpets the "environmental pollution" allegedly caused by the Second Lebanon War. Its website was set up in 2008 and has not been updated since.

xi) **Websites distributing anti-Israeli and anti-Semitic books**: Hezbollah formerly had a website for its publishing house, **Dar Al-Hadi**, which distributed anti-Israeli and anti-Semitic books. **Dar Al-Hadi** was closed, but the books published by Hezbollah (including Iranian books translated into Arabic) **are still offered for sale on Arab book sites and by Western sites abroad, including in the United States** (whose target audience, in our assessment, is Arabs/Muslims living there).

Selling Hezbollah Publications in the United States

xii) **Website of the Association of Imam Khomeini Cultural Centers in Lebanon**, an institute with many branches in Lebanon

whose objective is to spread the ideology of the Ayatollah Khomeini throughout Lebanon.

xiii) **The ShiaWeb**, which deals with Shi'ite theological issues. It has a link to a site affiliated with Hezbollah.

xiv) **Other websites** linked through the Society of Knowledge (Al-Maaref) website which deal with spreading Khomeini's ideology in Lebanon.

4) **Category 4 – Sites of municipalities in south Lebanon affiliated with Hezbollah** include the Shi'ite villages of **Bint Jbeil, Al-Taybeh and Jebchit**. They are three large Shi'ite villages in south Lebanon, two near the Israeli border and one in the Nabatieh Heights. The objective of their websites is to strengthen the ties between Hezbollah and these three important villages: **Jebchit** is the Hezbollah stronghold in the south Lebanon and **Bint Jbeil** has become a symbol of the so-called "resistance" to Israel. In addition, **Deir Qanoun al-Nahr** also has an active website affiliated with Hezbollah, although that is not specifically stated.[6]

5) **Category 5 – Websites dedicated for fostering the personality cults of senior Hezbollah figures**: The **Somod** ("firm stance") website, linked through the pro-Iranian Shi'ite ShiaWeb portal, focuses on the personality cult of **Hassan Nasrallah**. In addition, there is a Hezbollah-affiliated site for forums called "**the site of the admirers of the Sayeed Hassan Nassrullah**." **His second in command, Sheikh Naim Qassem**, has a personal site. Formerly there was a site of forums called **Abu Hadi**, a nickname of Nasrallah, but it is no longer active. Nasrallah's personal website as well, which appeared under the title "the website of the official representative in Lebanon of the Imam Khamenei" is also no longer active.

6) **Category 6 – Forums affiliated with Hezbollah**: The forums affiliated Hezbollah include **Qawem** ("resist!"), **Lebanon Chat** and the **Admirers of Sayeed Hassan Nassrullah**.

7) **Category 7 – YouTube and the social networks**: Hezbollah is very active in uploading propaganda videos to **YouTube** and in tweeting on **Twitter**. Facebook has imposed limits on Hezbollah since the summer of 2012. Hezbollah also uses **smartphone apps** (Apple's iPhone and Google's Android), although it encounters difficulties (because of the limits the United States places on Hezbollah, designated as a terrorist organization by the American administration).

18. **There is also a category of news sites which do not belong to Hezbollah but are affiliated with it and disseminate its propaganda**. They include:

1) **Al-Akhbar** is the website of a leading Lebanese newspaper, published in Beirut since 2006. The site does not belong to Hezbollah but is affiliated with it and consistently supports both Syria and Hezbollah; Hezbollah uses it as a platform to publish news items it wants to see in print.

2) **Al-Mayadeen** is the website of a Lebanese TV channel which began broadcasting in June 2012 as an alternative to Al-Jazeera TV and Al-Arabiya TV. It was founded by **Ghassan bin Jiddo**, formerly a senior Al-Jazeera correspondent and affiliated with Hezbollah. Hezbollah uses Al-Mayadeen as a platform to publicize articles, sometimes exclusively.

Op-Ed: Underwater Internet Cable Cutting in Cyber Warfare

By Eado Hecht

Source:http://www.israelnationalnews.com/Articles/Article.aspx/13182#.UXYzhEqdI11

Cyber warfare is the newest addition to the domain of war against Israel. Though attention is usually focused on software aspects of this new battlefield, a low-tech attack on the hardware infrastructure can be much more crippling and long-lasting.

In recent years there has been considerable discussion of the new phenomenon of cyber warfare, its methods, and its ramifications.

In essence there are three objectives that can be achieved by cyber-offensive activities: espionage (infiltrating the target's information

storage systems and stealing information), denial of service attacks (preventing Internet usage), and sabotage (infiltrating systems reliant on Internet connections and causing functional damage via malevolent programs).

The media largely focuses on the use of computer programs as weapons in the cyber domain, but an attack on Internet infrastructure is no less an option for terrorists, and often more devastating and effective. It doesn't require a great deal of computer programming skill to implement, and its effect is widespread and immediate. Even partial success has extensive consequences because of the resultant jamming of traffic on the limited remaining connection.

For example, on March 27, 2013, an Egyptian Navy patrol discovered and arrested three men engaged in cutting an underwater cable connecting Egypt to international internet service. Seacom, the cable operator, said that while the attack was interrupted before the cable had been completely cut, network speed was significantly reduced in Egypt. This was just one of many instances from over the past decade in which cables off the coast of Egypt were cut.

Underwater Cable Cutting

Submarine communications cables convey approximately 99 percent of inter-continental communications traffic, with the remaining 1 percent conveyed with reduced quality and efficiency by satellites. Originally these cables were electromagnetic, but since 1988 have been gradually replaced by fiber-optic cables.

Cables have been cut by nature (earthquakes, currents, and even shark bites) but mostly by human-caused accidents (trailing anchors or fishing nets) as well as deliberate military or criminal activity (stealing and selling sections of cable).

In fact, damage to cables is quite common, with several dozen up to a few hundred incidents per year. The response to this, in addition to technical improvements such as burying the cables and conducting repairs, has been to manufacture redundancy into the system, allowing for multiple cables to connect to different points by separate routes. This process has been improved by having a number of junctions connecting parallel cables, thus enabling the bypassing of specific sections that have been cut by transferring the traffic *en route* to other cables.

However, there are still weaknesses in various areas of the global layout of the network that can result in a particular client-area being cut off from service or suffering varying levels of service degradation.

For example, in January 2008 two cables were cut near Alexandria, Egypt, resulting in a severe disruption of Internet services in regional states. In February 2012, about half of the Internet networks in Kenya and Uganda were cut off from the world. That the more vulnerable areas (Africa, south central Asia, South America) and less vulnerable areas (North America, Europe, east Asia) are in line with the areas' economic status is not surprising; laying and maintaining the cables is extremely expensive.

Targeting international communication cables is not new. On August 5, 1914, the first military action by Great Britain after declaring war on Germany was to send the cable steamer '*Alert*' to cut Germany's five trans-Atlantic submarine telegraph cables. Similar actions by other British ships cut other sections of Germany's international telegraph communications with the rest of the world.

To communicate with its embassies, colonies, and naval bases around the world Germany was forced to rely on other means, specifically the telegraph services of neutral states. However, most of the non-German cables connecting Europe to the rest of the world had to pass through a British relay station and were thus vulnerable to eavesdropping.

This had a major strategic effect on the conduct of the war, when in January 1917 the British intercepted and decoded a telegram from the German government to the Mexican government proposing that Mexico should declare war on the United States. The Germans hoped that fighting with Mexico would keep the United States from involving itself in the war in Europe. This telegram, known historically as the "Zimmerman Telegram," was one of the catalysts for the US declaring war on Germany in 1917.

The Challenge for Israel

Until recently Israel had only one major cable connecting its Internet to the world; thus every malfunction immediately impacted on Israel's economic and private use. Redundancy was achieved only via satellite communications, though well below the requirement.

Though today there is a second parallel system which provides sufficient protection from natural or accidental incidents, a deliberate attack – similar to that of the British Navy on Germany's telegraph network – has a simple target.

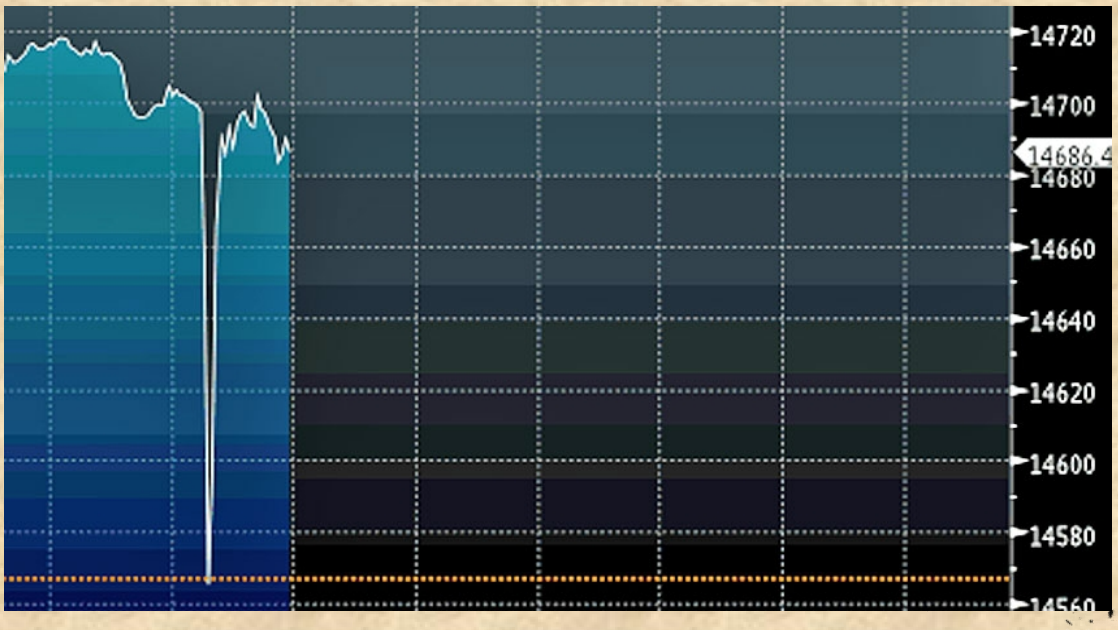
These cables require active protection measures if Israel is to prevent severance from the international Internet. In 1914 the British attack mainly affected Germany's diplomatic and military capability, and Germany had sufficient, if vulnerable to eavesdropping, alternatives. Today, the diplomatic and military effects of having Internet communication with world at-large cut off would be negligible, but the direct and indirect economic consequences could be extremely expensive to Israel's economy, especially with the transfer of much data to online cloud services that are actually placed abroad.

Defending against the new threat means adding a new mission to the Israeli Navy; however, there is no need for vastly increased naval resources to fulfill this mission. The Israeli Navy has for decades been monitoring the activity of vessels in Israel's vicinity for potential terrorist activity, and the navy recently beefed up its security capabilities to protect its new maritime gas-production facilities from various terrorist and military threats.

Therefore, the important factor is increased awareness and adapting existing maritime surveillance to ensure that the Internet cable routes are properly covered as well. A secondary necessity is a rapid repair capability, which is in any case the purview and interest of the cable companies themselves and only needs government supervision and naval escort (in times of war) to ensure a swift response.

Dr. Eado Hecht *is an independent defense analyst specializing in military doctrine and its interpretation. He teaches military theory and military history at Bar-Ilan and Haifa Universities and at the IDF Command and General Staff College, and serves on the Editorial Advisory Panel of The Journal of Military Operations.*

A new method of cyberterrorism?



April 23, 2013

Five tools to protect your privacy online

By Simon Black

Source: http://www.sovereignman.com/personal-privacy/five-privacy-tools-10859/

We've discussed many times before—**hardly a month goes by without some major action against Internet users**… from Obama's 'kill switch', to ACTA, SOPA and PIPA, to stasi tactics against people like Kim Dotcom.

Online privacy is becoming more important by the day. And nobody is going to give it to you, you have to take steps yourself to secure it.

Below are five different tools and services that will get you started:

1. Tor Browser

Tor is a great weapon in the fight for online anonymity as it allows you to surf the web without giving up your location and other personal data to the websites you visit.

The Tor Browser Bundle is the easiest and most secure way to get started; simply download it, and start surfing the web with the Tor Browser. It's available for Windows, Mac, and Linux.

2. Duck Duck Go

If you want privacy, don't search with Google.

Google store all of your searches to customize ads for you, but even worse, they can hand over the whole list of searches to any government agency that are curious about what you've been looking at for the last couple years.

A better alternative is Duck Duck Go, a completely anonymous search engine that does not store any information about you or your searches. The search results are essentially identical to Google's, so there's no loss of quality.

3. HTTPS Everywhere

HTTPS Everywhere is a plug-in for Firefox and Google Chrome that tries to force a website to connect in secure mode, thus encrypting your traffic with the website you are visiting. This makes your browsing more secure because it prevents eavesdropping thieves or state-mafia from intercepting your unencrypted Internet traffic.

4. Cryptocat

Cryptocat is an encrypted chat that beats Facebook and Skype when it comes to security and privacy. If you want to chat in private then this is one simple solution. It's also open source, which means you can see the full code and be sure there are no government "backdoors" built in.

5. Silent Circle

Silent Circle is a new player on the market, but it is founded by "old" players in the security and encryption industry. One of the founders, Phil Zimmerman, is also the creator of PGP, one of the most-used encryption platforms in the world.

Silent Circle is a suite of products offering:

- Encrypted email
- Encrypted video chat
- Encrypted phone calls
- Encrypted text messaging

Silent Circle is the only service on this list that is not free. But having the gold standard of encryption may be worth it for you. It is for me.

Bottom Line

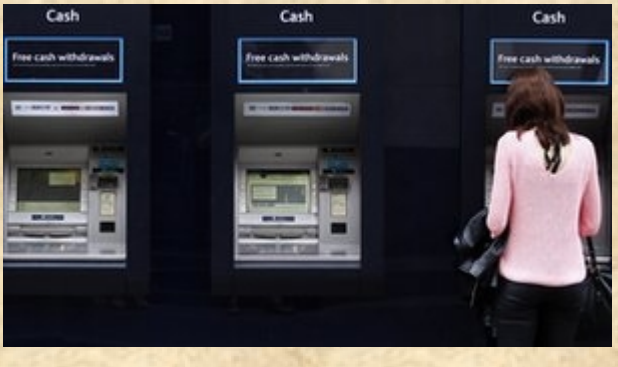
You can set up most of the tools we discussed in 5 minutes. Each of them will go a long way in securing your privacy online.

Is UK doing enough to protect itself from cyber attack?

By Mark Urban

Source: http://www.bbc.co.uk/news/uk-22338204

In 2010 the British government designated the protection of computer networks as one of the country's most important national security priorities. In its Strategic Defence and Security Review (SDSR) it pledged, "the National Cyber Security Programme will be supported by £650m of new investment over the next four years".



What exactly has this investment bought, three years on?

Speaking on and off the record to insiders - from the government, intelligence agencies and security industry - it is apparent that the achievements in defending the UK from this threat have disappointed many.

Much of the available funding may actually have been directed at improving the UK's ability to target other countries' computer secrets.

Critical national infrastructure could be affected if computer networks are not properly defended

Some point out that even if everything had gone to plan, an investment averaging £162.5m per year over four years could only have a limited effect on such a huge problem.

Security experts estimate that there are about 50 million cyber attacks a year in the UK, a number which they say is growing rapidly all of the time, and they put the damage to the UK economy at up to £27bn last year.

Yet, even according to government plans, less than half the total money committed has so far been spent.

Some of the things that have resulted from the government's investment

- The Serious Organised Crime Agency (SOCA) took down 36 website domains that sold credit card data
- 15,000 fraud websites were suspended
- GCHQ announced a scheme to help companies deal with cyber attacks and give guidance on response to a compromise
- Eight universities have been awarded Academic Centre for Excellence in Cyber Security and Research status for conducting world class research in cyber security
- The Cyber Security Information Sharing Partnership (CISP) is to be launched

There are suggestions that early strategising consumed many precious months and that the Cabinet Office, which is supposed to be giving overall direction to the project, has not yet allocated much of the money to specific projects.

"Some people have… said we're saving money for a rainy day," Mark Phillips, who helped draught the government's strategy, and is now at the Royal United Service Institute (RUSI) think tank, says. "To which my response is that we already have a rainy day, we have a high threat already with cyber."

Francis Maude, the minister responsible for cyber security, disputed this interpretation in a statement to BBC Newsnight, saying:

"Far from abdicating our responsibility on funding, to date we have spent over one third in the first two years of the programme. We are on target and in line with our public spending forecasts. The rapidly changing nature of cyber threats to the UK demonstrates the need for a flexible cyber security response so we reassess our spending priorities on a regular basis as was always the case. This is a prudent, sensible, smart approach as we move forward into the final two years of the programme."

Even if the full £650m is spent, as those close to the policy insist it will be, it is apparent that this will be done over five years rather than the originally promised four.

The other striking thing about the capability that has been taking shape is its offensive character; official figures show that 59% of the planned spend is meant to go to the intelligence agencies.

"We can achieve a tremendous amount these days through remote exploitation rather than face to face meetings with agents," says an MI6 officer referring to attacks on computer networks.

"GCHQ's offensive capability gives the UK an edge," a former senior officer at the eavesdropping centre in Cheltenham told me, adding, "a large proportion of that money has [therefore] gone into those capabilities".

John Bassett, now at RUSI and formerly GCHQ's Senior UK Liaison Officer in Washington, adds that much of the new government funding has gone on, "existing programmes... designed to get a really strong grip on global situational awareness".

Is this just a polite way of referring to stealing others' secrets?

Mr Bassett suggests that understanding the threat to UK computer security requires the exploration of adversary capabilities.

This argument, that the UK's defence requires the penetration of other countries' computer networks makes it hard to define whether most of the British cyber-security spend is actually going on offensive work - hacking for want of a better term - or whether that activity only accounts for some of it.

However, everybody one speaks to within the circle of secrecy assumes that this type of activity has consumed a significant proportion, measurable in the tens of millions, of the UK's total spending on cyber elements.

That emphasis on offensive work is remarkable given that the SDSR and the government cyber security strategy published in 2011 explained the rationale for the new spending almost entirely in terms of protecting the UK economy and government from attack.

Indeed, at an SDSR press briefing in 2010 a senior government official who I asked whether the UK even had an offensive cyber programme declined to confirm that it did, although another official subsequently contacted me to say that there was such an effort.

Mark Phillips, who was present at many of the meetings that formulated both policies, told us that the offensive programme was "one of the two unstated objectives" of the cyber security plan. The other, he implied, was providing support to allies, which in an intelligence context is usually taken as a reference to the US.

Nightmare scenarios such as hijackers taking control of an aircraft via its computerised systems, or shutting down a national power system or a country's entire internet, appear feasible... To what extent such risks are exaggerated by security firms touting for business is open to argument"

The UK Ministry of Defence (MoD) meanwhile has taken 14% of the new money for cyber security, spreading it more or less evenly between offensive and defensive roles, insiders suggest.

It has launched Project Watchtower - a series of programmes designed to crated a super secure cyber architecture for the MoD -in an attempt to secure the military's computer networks from sophisticated attacks, with experts suggesting some good progress has been made.

On the offensive side, the MoD has established its Joint Cyber Unit, based at Cheltenham. The impetus for the creation of this outfit, several dozen strong, came from Nato's bombing campaign in Libya, says one Whitehall player.

Ministers asked why the MoD did not have the capability to switch off the Libyan air defence system from afar by means of cyber attack.

One MoD insider argues that the UK is some way from being able to take action of this kind, or match the unleashing of the Stuxnet virus on Iran's uranium enrichment plant, widely believed to have been carried out by the US, although they have not officially admitted it, but that the hold-up is on the policy and legal front rather than the issue of technical ability.

There has been a lively discussion among Whitehall law officers about whether the use of such a cyber attack would constitute an act of war or could under certain circumstances, for example switching off power to a hospital, be construed as a war crime.

Increasingly it is in this area, the development of cyber weapons or disruptive malware, rather than in the long established game of stealing secrets - state or commercial - that attention is focussing in the security community.

In 2011-12, for example, the US Department of Homeland Security tracked 23 cyber attacks on companies related to the national gas pipeline system. They assessed that the targeted information would have allowed an intruder to blow up hundreds of compressor stations, blacking out the US energy grid, "at the click of a mouse". Oil installations in Iran and Saudi Arabia have also had their control equipment hit by malware.

Mr Maude stressed to us that the UK's programme is "not just about securing government systems, though it helps do that too, but underpins all our objectives in tackling cyber crime, protecting our critical national infrastructure and making the UK one of the safest places in the world to do business in cyberspace." He noted that the Economist Intelligence Unit has put Britain top among the G20 countries for creating a secure environment for networks.

Notwithstanding this accolade, there is widespread concern about the vulnerability of the UK's national infrastructure to attacks of this kind.

"I don't think anyone is any more secure than they were," said Rashmi Knowles, Chief Security Architect at RSA, a leading cyber security firm, when I asked her whether Britain's infrastructure is any better protected than when the government launched its initiative in 2010.

In part this stems from constant evolution of the threat, with hackers far more dynamic, constantly evolving new techniques, than the government bureaucracies that try to stop them. As for the work that has been done to thwart them, some sectors, such as banking, have a far greater interest in investing in secure networks than the likes of public utilities.

Nightmare scenarios such as hijackers taking control of an aircraft via its computerised systems, or shutting down a national power system or a country's entire internet, appear feasible in the light of the US gas pipeline case. To what

extent such risks are exaggerated by security firms touting for business is open to argument.
What almost all parties in the cyber security sector agree is that awareness of the risks is growing. For the government experts trying to devise a response, the risk is that their solutions may be judged inadequate to the scale of that challenge.

Mark Urban is diplomatic and defence editor, Newsnight.

Cyber Trainer prepares Cyber Warriors for the digital battlefield

Source: http://i-hls.com/2013/05/elbit-systems-cyber-trainer-prepares-cyber-warriors-for-digital-battlefield/

Elbit Systems (Israel) works intensively on developing expertise also in the virtual arena, focusing on providing a "protection shield" in the Cyber field for countries interested in defending their computer networks. Having invested tens of millions of dollars in the field,

Elbit developed a simulator for Cyber defense, training teams in defending large scale computer networks of governmental and military organizations, infrastructure companies and large financial organizations.
There are already several customers using the simulator, in Israel and abroad.
The new simulator exposes the cyber defenders to a variety of situations and scenarios simulating a real cyber attack. The simulator enables individuals and groups to experience virtual cyber events and attacks, while helping them to locate the danger, to cope with it, and to manage and handle the situation. It helps trainees to learn how to protect themselves from future attacks by experiencing networks defense by simulation. At the end of the drill, similarly to flight simulation, the trainer enables investigation of the just finished cyber defense activity and drawing conclusions while maintaining a documented follow up of the trainees` progress during a whole sequence of training sessions. In this way it is possible to sharpen and improve the capabilities of the trainee – for correct functioning during a real cyber attack in real time.
The technology developed by Elbit Systems in the recent years in the field of cyber command and control and defending the cybernetic space attracts much attention by various bodies worldwide preparing for possible cyber attacks. The customers are interested in various versions of cyber simulator and two versions were already sold and supplied to customers in Israel and abroad. As for today, Elbit Systems has several orders in the field of Cyber, with a scope of millions dollars, and the future potential is enormous. 120 countries are engaged nowadays in a cyber arms race, and the budgets of governments, armies and infrastructure organizations dedicated for the subject are growing dramatically.
In the last three decades, Elbit Systems acquired a lot of experience in training and simulator systems, making a maximal use of its advanced C3 (communications, command and control) capabilities, and of the operational experience of pilots, tank commanders and ship commanders.
Recently, the company introduced an innovative concept – "Connected Trainers" – enabling training of pilots in a structured formation of operational flight, combined with

other, land and airborne, forces. This concept is being introduced to the training program of the Israeli Air Force, as part of a giant project of development and implementation of a mission training center for the "Barak" (F-16C/D) and "Soofa" (F-161) airplanes of the IAF.

In parallel, Elbit offers a "live training" system intended for training of a brigade battle team including infantry, armored forces and land assistance (artillery and air defense). The live training includes virtual components for enrichment of battlefield display, and video capabilities for improved control and interrogation. Training at the field, using operational weapons and platforms without using live ammunition, enables the trainee to acquire experience and skill in field conditions while saving training time and ammunition costs.

Eight New Yorkers charged over $45 million cyber-attack

Source:http://www.irishtimes.com/news/world/us/eight-new-yorkers-charged-over-45-million-cyber-attack-1.1388640

Eight New York residents were charged in what US prosecutors said was a $45 million global debit card cyber-attack scheme targeting banks based in the United Arab Emirates and Oman.

The defendants are accused in a four-count indictment unsealed today in federal court in Brooklyn, New York, of participating in two worldwide attacks.

A woman looks at a map showing where eight members belonging to a New York-based cell of a global cyber criminal organization withdrew money from ATM machines, during a news conference in New York. Photograph: Lucas Jackson/Reuters

They used stolen account information for prepaid MasterCard-branded debit cards to withdraw millions of dollars from ATM machines from October 2012 to April 2013, prosecutors said.

The targeted banks were National Bank of Ras Al-Khaimah PSC, based in the United Arab Emirates, and Bank Muscat SAOG, Oman's biggest bank by assets, according to the US Attorney's Office in Brooklyn.

Participants in the scheme hacked into credit card processors to steal the card data and eliminate withdrawal limits, prosecutors said. They took out cash in coordinated efforts "reminiscent of the casino heist in 'Ocean's Eleven,'" Brooklyn US Attorney Loretta Lynch said in a news conference, referring to 1960 movie remade in 2001.

"Our message is clear. Law enforcement should not stand by as cyber criminals target our global financial system for their own ends," she said. The attack was the "largest theft of this type that we have yet seen," she said.

Defendant murdered

Seven of the individuals, who are residents of Yonkers, New York, have been arrested, prosecutors said. An

additional defendant charged in the scheme, Alberto Yusi Lajud-Pena, was reported to have been murdered in the Dominican Republic in April, prosecutors said.
The defendants are all charged with conspiracy to commit access device fraud and three are charged with money laundering. The defendants face a maximum of 10 years in prison for money laundering and 7.5 years for conspiracy, according to prosecutors.
In February, Bank Muscat announced that 12 of its prepaid travel cards were compromised in a fraud totaling $39 million (15 million Omani rials).

Top Ten Hacking Countries

Source: http://www.bloomberg.com/slideshow/2013-04-23/top-ten-hacking-countries.html

When it comes to computer-attack traffic, China deserves the bulk of the blame, but not all of it.
Ten countries including China accounted for three-quarters of the world's cyber-assault traffic during the last quarter of 2012, according to Akamai Technologies, which helps companies speed the delivery of online content.
While detecting the source of an attack can be difficult -- cyber criminals can launch online assaults from infected computers around the world -- knowing the country of origin can provide an important clue in ultimately determining the identity of a hacker.

10. Hungary
Hungary accounted for 1.4 percent of the world's attack traffic in the fourth quarter of last year, putting the country in 10th place. It narrowly beat out South Korea. Hungary's percentage was unchanged from the previous and year-ago quarters.

9. Italy
Italy accounted for 1.6 percent of the world's attack traffic in the fourth quarter of last year, putting the country in 9th place. Italy's share decreased slightly from 1.7 percent in the previous quarter and 1.9 percent in the year-ago period.

8. India
India accounted for 2.3 percent of the world's attack traffic during the fourth quarter of last year, putting the country in 8th place. India's share decreased from 2.5 percent in the previous quarter and 3 percent in the year-ago period.

7. Romania

Romania accounted for 2.8 percent of the world's attack traffic during the fourth quarter of last year, putting the country in 7th place. Romania's share increased from 2.7 percent in the previous quarter and 2.6 percent in the year-ago period. Several news reports have described Ramnicu Valcea, a town in Romania, as a haven for cyber criminals.

year, putting the country in 4th place. Russia's share decreased from 4.7 percent in the previous quarter and 6.8 percent in the year-ago period. At least 40 companies including Apple, Facebook and Twitter were targeted in malware attacks linked to a cyber criminal group based in Russia or Eastern Europe, according to a recent Bloomberg News report.

6. Brazil

Brazil accounted for 3.3 percent of the world's attack traffic during the fourth quarter of last year, putting the country in 6th place. Brazil's share fell from 3.8 percent in the previous quarter and 4.4 percent in the year-ago period.

5. Taiwan

Taiwan, which is a province of China, accounted for 3.7 percent of the world's attack traffic during the fourth quarter of last year, putting the region in 5th place. Taiwan's share dropped from 4.5 percent in the previous quarter and 7.5 percent in the year-ago period.

While Taiwan is a top source of attack traffic, it is also a popular target. Research by the security firm Sophos found that 12.7 percent of computers in Taiwan had been attacked by malware during a three-month study last year.

4. Russia

Russia accounted for 4.3 percent of the world's attack traffic during the fourth quarter of last

3. Turkey

Turkey accounted for 4.7 percent of the world's attack traffic during the fourth quarter of last year, putting the country in 3rd place. Turkey's share increased from 4.3 percent in the previous quarter and fell from 5.6 percent in the year-ago period.

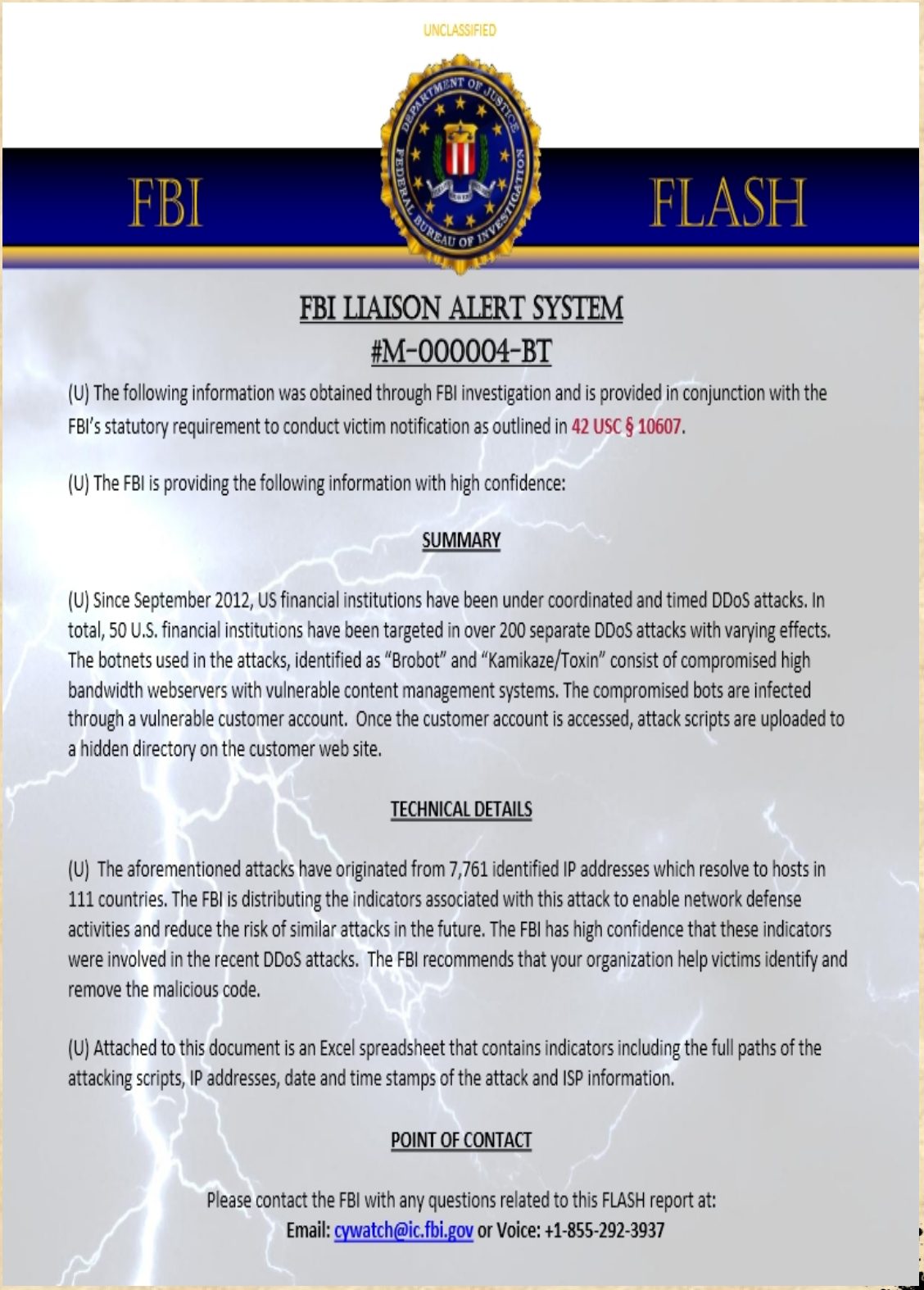
2. United States

The U.S. accounted for 10 percent of the world's attack traffic during the fourth quarter of last year, putting the country in 2nd place. The U.S.'s share dropped from 13 percent in the previous quarter and matched its percentage from the year-ago period. The U.S. is home to members of some of the world's most notorious hacker groups, including Anonymous and AntiSec.

1. China

China accounted for 41 percent of the world's attack traffic during the fourth quarter of last year, making the

country the top source of cyber assaults. China's share increased from 33 percent in the previous quarter and 13 percent in the year-ago period, according to Akamai. Investigations have discovered a sophisticated hacker network in China. Some members are connected to China's military, though the extent of these official operations is unknown. The government and its state-run media continue to deny China's involvement in international hacking incidents.



UNCLASSIFIED

FBI FLASH

FBI LIAISON ALERT SYSTEM

#M-000004-BT

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

(U) The FBI is providing the following information with high confidence:

SUMMARY

(U) Since September 2012, US financial institutions have been under coordinated and timed DDoS attacks. In total, 50 U.S. financial institutions have been targeted in over 200 separate DDoS attacks with varying effects. The botnets used in the attacks, identified as "Brobot" and "Kamikaze/Toxin" consist of compromised high bandwidth webservers with vulnerable content management systems. The compromised bots are infected through a vulnerable customer account. Once the customer account is accessed, attack scripts are uploaded to a hidden directory on the customer web site.

TECHNICAL DETAILS

(U) The aforementioned attacks have originated from 7,761 identified IP addresses which resolve to hosts in 111 countries. The FBI is distributing the indicators associated with this attack to enable network defense activities and reduce the risk of similar attacks in the future. The FBI has high confidence that these indicators were involved in the recent DDoS attacks. The FBI recommends that your organization help victims identify and remove the malicious code.

(U) Attached to this document is an Excel spreadsheet that contains indicators including the full paths of the attacking scripts, IP addresses, date and time stamps of the attack and ISP information.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at:
Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937

Wave of cyberattacks targets American energy companies

Source: http://www.homelandsecuritynewswire.com/dr20130513-wave-of-cyberattacks-targets-american-energy-companies

A new wave of cyberattacks has been hitting American corporations, and federal officials, say the attackers, who reside somewhere in the Middle East, are trying to sabotage these corporations.

The *New York Times* reports that the majority of the targets have been energy companies. The attacks are trying to take control of company's processing systems. Officials say they do not know whether the attacks are the work of criminals, hacking organizations, or are state-sponsored.

"We are concerned by these intrusions, and we are trying to make sure they don't lead to something much bigger, as they did in the Saudi case," one senior American official told the *Times*.

Two senior officials say the attacks were focused on the system of ten American energy firms. DHS has since released a warning describing the attacks as "probes that suggest someone is looking at how to take control of these systems."

Last week's warning "is an effort to make sure that the volume and timeliness of the information improves," in line with a new executive order signed by the president, one senior official said.

The warning was issued by ICS-CERT, a federal agency which keeps an eye on attacks on computer system that run industrial processes. The agency says that the government has been "highly concerned about hostility against critical infrastructure organizations."

The warning pressed chemical and energy companies to take steps to protect their systems. Dan McWhorter, the managing director of threat intelligence at Mandiant Corporation, said the suggestions DHS outlined were for "things most everyone should be doing on an everyday basis.

The warnings have unintentionally highlighted the fact that cellphone networks, electric utility grids, and chemical companies are not run by the government but by private organizations.

"The challenge will be managing our nation's offensive and defensive capabilities," said Evan Wolff, a partner at Hunton & Williams, who runs the firm's homeland security practice and focuses on cyber issues. "Unlike conventional weapons, this will require a very broad engagement across the private sector."

DHS has spent the last several years trying to boost its cybersecutiry force in an effort to keep up with the increasing number of attacks, but that effort has been hampered by top officials leaving.

Jane Holl Lute, the agency's deputy secretary, Mark Weatherford, the department's top cybersecurity official, Michael Locatis, the assistant secretary for cybersecurity, and Richard Spires, the agency's chief information officer, have all left their positions recently.

Internet Crime 2012 - IC3 Releases Annual Report

Source:http://www.fbi.gov/news/stories/2013/may/internet-crime-in-2012/internet-crime-in-2012?utm_campaign=email-Immediate&utm_medium=email&utm_source=fbi-top-stories&utm_content=224677

The Internet Crime Complaint Center, or IC3, had received dozens of complaints about a St. Louis woman who was selling what she claimed were designer handbags. Buyers spent as much as $100,000 for a single bag, but ended up with either knock-off bags or sometimes nothing at all…and the woman refused to refund their money. The IC3 forwarded the complaints to the St. Louis FBI Field Office, and

after an investigation, the woman was charged with selling counterfeit goods and ultimately pled guilty last year.

This case is an example of the effectiveness of

the IC3—a partnership between the FBI and the National White Collar Crime Center. Submissions to this central hub for Internet-related crime complaints can not only lead to culprits getting caught, but also help identify trends that are then posted on the IC3's website to educate the public about constantly evolving cyber threats and scams.

Today, as part of its ongoing education and prevention mission, the IC3 released its latest annual snapshot of online crime and fraud—the *2012 Internet Crime Report*. While there is no end to the variety of cyber scams, the report highlights some of the most frequent ones from 2012. Here are a few examples of what to look for to help keep you from being victimized:

- **Auto fraud:** Criminals attempt to sell vehicles that they really don't own, usually advertising them on various online platforms at prices below market value. Often the fraudsters claim they must sell the vehicles quickly because they are relocating for work, are being deployed by the military, or have a tragic family circumstance and are in need of money. And in a new twist, criminals are posing as dealers rather than individual sellers.
- **FBI impersonation e-mail scam:** The names of various government agencies and government officials have been used in spam attacks for some time, and complaints related to spam e-mail purportedly sent by the FBI continue to be reported with high frequency. These scams, which include elements of Nigerian scam letters, incorporate get-rich inheritance scenarios, bogus lottery winning notifications, and occasional extortion threats.
- **Intimidation/extortion scams:** More popular ones involve payday loan scams (harassing phone calls to victims claiming they are delinquent on loan payments); process server scams (a supposed process server shows up at a victim's house or place of employment but is willing to take a debit card number for payment in order to avoid court); and grandparent scams (fraudsters contacting elderly victims pretending to be a young family member in some sort of legal or financial crisis).
- **Scareware/ransomware:** There are different variations of these

Report Highlights

- The IC3 received nearly 290,000 complaints from victims.

- Dollar losses arising from the 2012 complaints totaled almost $525.5 million.

- Most complaints came from the U.S., but some were sent from Canada, the United Kingdom, Australia, India, and other countries.

- California had the highest percentage of complaints (13.41), followed by Florida, Texas, New York, New Jersey, Pennsylvania, Illinois, Virginia, Ohio, and Washington.

- Victims who reported losing money lost an average of nearly $4,600.

- More than 82 percent of complainants were ages 20-50, while 14 percent were 60 and over, and just over 3 percent were under the age of 20.

Fraud Advice for Consumers

- Be suspicious if the seller only accepts wire transfers or cash.

- If purchasing merchandise, ensure it is from a reputable source.

- Be wary of businesses that operate from P.O. boxes or mail drops.

- If you receive an unsolicited e-mail, be very cautious when responding to offers and giving out personal or financial information. Also, do not click on the links in these e-mails; instead, go directly to the organization's official website.

For more tips, go to the IC3's *2012 Internet Crime Report* and our Internet Fraud webpage.

scams, but one involves victims receiving pop-up messages on their computers alerting them to purported infections that can only be fixed by purchasing particular antivirus software. Another involves malware that freezes victims' computers and displays a warning of a violation of U.S. law and directions to pay a fine to the U.S. Department of Justice.

Read more on these and other scams—as well as online crime prevention tips—in the IC3's latest report. An educated consumer is the most effective weapon against Internet fraudsters.

► **Read the full report at:** http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

► **Source**
http://www.floridatechonline.com/lp/all/prestige/grad-mba_cybersecurity_t10_1304/?source=199772zf1&mcguid=0df5914e-d8ed-434b-9ab3-97869cbc5273&mcid=24103

New software protects networked control systems from cyber attacks

Source: http://www.homelandsecuritynewswire.com/dr20130514-new-software-protects-networked-control-systems-from-cyber-attacks

Researchers from North Carolina State University have developed a software algorithm that detects and isolates cyber-attacks on networked control systems — which are used to coordinate transportation, power, and other infrastructure across the United States.

Networked control systems are essentially pathways that connect and coordinate activities between computers and physical devices. For example, the systems that connect temperature sensors, heating systems and user controls in modern buildings are networked control systems.

A North Carolina State University release reports that on a much larger scale, however, these systems are also becoming increasingly important to national infrastructure, such as transportation and power. Because they often rely on wireless or Internet connections, these systems are vulnerable to cyber-attacks. "Flame" and "Stuxnet" are examples of costly, high-profile attacks on networked control systems in recent years.

As networked control systems have grown increasingly large and complex, system designers have moved away from having system devices — or "agents" — coordinate their activities through a single, centralized computer hub, or brain. Instead, designers have created "distributed network control systems" (D-NCSs) that allow all of the system agents to work together, like a bunch of mini-brains, to coordinate their activities. This allows the systems to operate more efficiently. And now these distributed systems can also operate more securely.

The release notes that NC State researchers have developed a software algorithm that can detect when an individual agent in a D-NCS has been compromised by a cyber-attack. The algorithm then isolates the compromised agent, protecting the rest of the system and allowing it to continue functioning normally. This gives D-NCSs resilience and security advantages over systems that rely on a central computer hub, because the centralized design means the entire system would be compromised if the central computer is hacked.

"In addition, our security algorithm can be incorporated directly into the code used to operate existing distributed control systems, with minor modifications," says Dr. Mo-Yuen Chow, a professor of electrical and computer engineering at NC State and co-author of a paper on the work. "It would not require a complete overhaul of existing systems."

"We have demonstrated that the system works, and are now moving forward with additional testing under various cyber-attack scenarios to optimize the algorithm's detection rate and system performance," says Wente Zeng, a Ph.D. student at NC State and lead author of the paper.

The paper, "Convergence and Recovery Analysis of the Secure Distributed Control Methodology for D-NCS," will be presented at the IEEE International Symposium on Industrial Electronics, 28-31 May, in Taipei, Taiwan.

The research was funded by the National Science Foundation

.

"Convergence and Recovery Analysis of the Secure Distributed Control Methodology for D-NCS"

Authors: Wente Zeng and Mo-Yuen Chow, North Carolina State University

Presented: May 28-31, IEEE International Symposium on Industrial Electronics, Taipei, Taiwan

Abstract

Distributed control algorithms (e.g., consensus algorithm) are vulnerable to the misbehaving agent compromised by the cyber-attacks in Distributed Networked Control Systems (D-NCS). In this paper we continue our work on the proposed secure distributed control methodology that is capable of performing a secure consensus computation in D-NCS in the presence of misbehaving agents. The methodology is introduced first and proved to be effective through the convergence analysis. We then extend our

secure distributed control methodology to the leaderless consensus network by introducing and adding two recovery schemes into the current secure distributed control framework to guarantee the accurate convergence in the presence of misbehaving agents. All phases in our method are distributed in the sense that at each step of the detection, mitigation, identification, update and recovery, every agent only uses local and one-hop neighbors' information. The simulation results are presented to demonstrate the effectiveness of the proposed methods.

Emerging Cyber Threats Report 2013

Source: http://gtsecuritysummit.com/pdf/2013ThreatsReport.pdf

Innovative research can help illuminate the security problems facing people, businesses, and governments online as well as propose and evaluate new defenses.

In the past year, much has changed in cybersecurity. Attackers aligned with national agendas have focused on targeting businesses and governments in attacks that have resulted in the leakage of sensitive and critical data. Employees bringing consumer technology into the workplace—most notably, smartphones and tablets—have led to increased productivity, but at the same time have undermined the security practices at companies which had, in the past, focused on securing their perimeter. The movement of business and consumer data to the cloud has often led to the increase of the overall security of such information but created large stores of important data that will lure attackers.

If we are going to prevent motivated adversaries from attacking our systems, stealing our data and harming our critical infrastructure, the broader community of security researchers—including academia, the private sector, and government—must work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it.

The annual Georgia Tech Cyber Security Summit (GTCSS) on November 14, 2012, provides an opportunity for these stakeholders to come together and prepare for the challenges we face in securing cyberspace and cyber-connected physical systems. By seeking to engage a broader audience, Georgia Tech remains at the center of efforts to develop new technologies and strategies that are effective against sophisticated cyber attacks

The Georgia Institute of Technology is one of the nation's leading public research universities. The Georgia Tech Information Security Center (GTISC), the Georgia Tech Research Institute (GTRI), and dozens of labs across campus are engaged in research efforts focused on producing technology and driving innovation that will help secure business networks, industrial controls, government systems, and people's data. As a leader in cyber security research, Georgia Tech focuses on developing novel solutions to solve important problems. Atlanta is a major hub for cybersecurity, and Georgia Tech has acted as an

incubator for many companies that have succeeded internationally.
The discussion starts here. As key stakeholders, we all need to cooperate more effectively to combat the large-scale threats we face today and keep pace with constantly evolving attacks. At Georgia Tech, we understand this and, leveraging in-house research and expertise, have compiled the following Emerging Cyber Threats Report, which includes insight and analysis from a variety of experts from the IT security industry and academia. The Report and the Summit provide an open forum for discussion of emerging threats, their potential impact, and countermeasures for containing them. We invite you to learn more about our work in cyber security and to connect with our experts to understand and address the challenges we face in securing cyberspace.

Wenke Lee
Director, GTISC

Bo Rotoloni
Director, Cyber Technology and
Information Security Laboratory, GTRI

Recent Banking Heist Highlights Need for Cyber Security

By Jayson DeMers
Source: http://technorati.com/technology/it/article/recent-banking-heist-highlights-need-for/

As the world watches what will prove to be the largest bank robbery in history unfold - cyber criminals were able to steal more than $45

million from banks all over the world - many see a problem far bigger than missing money. This is an attack that the world had never seen before and something that makes authorities very nervous.
Police are calling this attack “unlimited” as hundreds of associates were able to target victims in 26 countries and drain ATMs as well as turn some of the largest corporations in the world into victims. There were two attacks, the first was in December and walked away with more than $5 million USD. Then, in February, the hacked American credit giants Visa and Mastercard, pulling down a hefty $40 million USD. The relative ease and anonymity of these attacks highlights the need for increased cyber security at every level of society.

Evolution of a Battlefield

There are thousands of ways to launching a cyber attack also drive up the price of cyber defense: stealing passwords, accessing confidential data (such as account balances, e-mail addresses, etc.), even attempts to outright control a system all mean that there's no 'one size fits all' cyber security solution. Additionally, there are thousands of new viruses and worms developed on a daily basis, making cyber security an extremely volatile market.
There's no one program that can make an organization completely safe from every form of hacking or infiltration. The company with the best protection is one that has multiple layers of security on multiple fronts, to stymie every combination of attack from a would-be hacker. This, naturally, is easier said than done, and it is a lot more expensive, too.

Safe and Sound

Inconvenient as the new procedures will undoubtedly be, especially in the beginning while technology is advancing, there's one group of people who won't mind at all - the security industry, which not only deals with the design and production of metal detectors and hand-held wands, but also bolstering cyber security for companies from a local small business to Facebook and nationwide banks.
If, at some point in the past, cyber security was considered an accessory or a luxury, those days are long gone. "It is no longer a footnote

in the needs of supporting a business," says Frank Cilluffo, the director of George Washington University's Homeland Security Policy Institute.

Rising To The Challenge

As cyber attacks have increased in frequency - an incredible 782% from 2006 to 2012 - public companies, particularly financial institutions - have lost sleep thinking about new ways to protect their assets and customers' data from attacks by hacking groups or new age terrorists. In a few years' time, cyber security will become the second largest operational cost in the American market.

The Future of Cyber Security

Alexander Southwell, the co-chair of Gibson, Dunn & Crutcher predicts that digital attackers will become even more sophisticated, always maneuvering themselves to stay one step ahead of governments and law enforcement agencies, both sides locked in a long distance, virtual game of cat and mouse. By the end of this decade, spending on cyber security will cost more than $7 billion (a comparatively conservative estimate), as companies look to expand from traditional security services and law enforcement and government work overtime to stay one step ahead of very resourceful and very persistent digital criminals.

Southwell further predicts that the prevalence of smart phones and mobile technology, and the reliance on cloud computing for data storage and the actual conduct of business, will become weapons in this invisible war. As companies seek more innovative and direct ways to liaise with their customers, there will be people who try and take advantage of that. For all the benefits and features smartphones and cloud computing offer, the combination could prove disastrous in the hands of the wrong person with bad intentions.

***Jayson DeMers** is the founder & CEO of AudienceBloom, a Seattle-based SEO agency, as well as Crackerize.com, a lyrics-humor website.*

OAS Report Examines Cybersecurity Trends in the Americas

Source: http://www.thebahamasweekly.com/publish/oas-media-releases/OAS_Report_Examines_Cybersecurity_Trends_in_the_Americas28169.shtml

The Organization of American States (OAS) through the Secretariat of Multidimensional Security (SMS) and the Inter-American Committee against Terrorism (CICITE) released today the report "Latin American and Caribbean Cybersecurity Trends and Government Responses." Prepared in collaboration with the company Trend Micro, the report illustrates and analyzes

cybersecurity and cybercrime trends in the region. The document contains detailed information on cyberthreats in the Americas, and for the first time incorporates the perspectives and experiences of OAS Member State governments.

The Secretary General of the OAS, Jose Miguel Insulza, affirmed that "this research responds to the needs of regional governments to confront cybercrime, which is increasingly frequent and threatening, due to the accelerating evolution of technology." He added that "to evaluate and effectively combat cyber threats, countries need detailed and reliable threat information, which this report provides. It represents a significant advance, considering that a study like this has not yet been carried out in our region. Organized crime now utilizes modern technology and in certain cases these criminals have more resources at their disposal than countries can dedicate to scientific development. We need to change this."

The report found an overall increase in cyber attacks; an increase in "hacktivism," or politically motivated hacking; internet-assisted money laundering; and attacks against critical infrastructure. Other trends discussed include levels of malware, spam, and wire fraud.

Conclusions highlighted in the report signal a pressing need to "maintain parity with those seeking to exploit digital vulnerabilities." The lack of

resources dedicated to building cybersecurity capacity and the scarcity of specialized knowledge and experience needed to secure networks and implement effective policies are two of the things that the report cites as hindering information security.

In its conclusions, the report contends that "organized crime groups are increasingly cyber-capable and hacker groups are growing in number and sophistication." The activity of internet users in the region is also discussed. They often practice unsafe online habits, such as running unpatched operating systems or using unsecured mass storage devices. Overall, most internet users pay little attention to cybersecurity. Finally, the document discusses cybercriminals' use of banking trojans as opposed to malware that predominates in other parts of the world.

In its recommendations, the report urges countries to promote raising awareness of safe cyber practices; promoting and investing in technical education programs; strengthening mechanisms to designate governmental roles and responsibilities related to cybersecurity; and instituting norms for international information sharing and cooperation on cybersecurity and cybercrime issues.

As opposed to previous reports on cyber activity in the Americas, the OAS and Trend Micro report and analysis incorporates the perspectives and experiences of OAS Member State governments. The OAS invited its Member States to contribute qualitative and quantitative information to the report regarding instances of hacking, cybercrime, and government efforts. 20 out of 32 Latin American and Caribbean Member States responded to the request to provide information. Trend Micro gathered technical data on malicious web traffic and hacking trends.

The Secretary of Multidimensional Security of the OAS, Adam Blackwell, said that the report "presents an opportunity for governments to showcase what types of initiatives have been successful in mitigating cyber risk. Ultimately, the insights and analysis that came from my team's extensive research will provide a valuable resource to those working to secure our vital networks. I would finally like to highlight that this joint effort represents the type of public-private cooperation that our Member States have recognized as pivotal to achieve sustainable hemispheric security."

The Vice President of Cyber Security of Trend Micro, Tom Kellermann, also highlighted some of the key findings of the report. "Latin America and the Caribbean regions are experiencing rapid technological adoption. But with this evolution comes the dark side of globalization - cybercrime." He added that, "this seminal report depicts the growth of web based attacks as well as the use of online forums for hosting and money laundering. Achieving sustainable economic growth in the region will be dependent upon a concerted regional effort to strengthen cybersecurity and combat cybercrime."

Protection against cyberthreats has become a major security concern worldwide. Since 2004, the OAS through the Inter-American Committee against Terrorism has worked to develop and enhance the capabilities of Member States to prevent and combat threats to cybersecurity at the national and regional levels.

CyberSecurity Still Lagging Behind

Source: http://www.acdemocracy.org

If you are one of some 600,000 subscribers to the Financial Times, you may wish to change your account's password.

Earlier today, a few of the paper's Twitter accounts and a blog were compromised by Bashar Assad's thugs, bragging on their Twitter, "**Hacked by the Syrian Electronic Army**."

Earlier the FT reported that a member of the Syrian Electronic Army was interviewed by the paper's reporters via email, and that the hacking was facilitated by phishing attacks on some of the FT's email accounts. Yet no link was made between that correspondence, which exposed FT email accounts, to today's hacking.

In what can best be described as English subtlety, the article describing the attack did not even made headlines on the FT's home page. "We have now locked those accounts," announced the FT official, who praised Twitter's help.

Nothing was said about the paper's subscribers' accounts. Clearly, the new two-step authentication that Twitter was supposed to establish, after the Associated Press account was hacked last month, failed.

Phishing, hacking emails, stealing passwords and compromising whatever and whoever is linked is not the only threat our cyber communications is facing today.

Discoveries that computers--used by governments, industries financial institutions and everything else--have been infected by malware, either imbedded in software or through the Internet, don't make headlines anymore. The damages that are reported are huge, but most still go unreported and possibly have not yet been discovered and therefore the real cost is unfathomable.

While these discoveries demonstrate that security experts are catching up, it's too little, too late. While protecting our cyber communication channels from stealth predators though the Internet is challenging, we could and should prevent the planting of malware in software by carefully vetting the designers.

However, software developers often seem more concerned with their bottom line and are cutting cost by employing cheap, unvetted labor. While their revenues may well increase, the cost to the economy and national security could be devastating.

Most public and private entities rely on and are dependent upon by the government for timely warning and for identifying the attackers after an attack. To better protect the critical infrastructure against cyberattack, DHS has contracted Northrop Grumman to begin the security accreditation process that's required before approval to operate as a commercial services provider under the Department's Enhanced Cybersecurity Services program.

Major private sector entities would like the government to allow them to take preventive offensive tactics against cyber attacks. Since the government prevents such measures, "Bank representatives on the Federal Advisory Council said at their last gathering on Feb. 8 in Washington that the Fed should collect and distribute threat information to lenders, law enforcement, securities exchanges and clearinghouses," according to Bloomberg. A number of banks recently asked the Federal Reserve to take the lead in defending the financial services industry from cyberattacks by working with federal counterterrorism, intelligence, and law enforcement agencies.

The government, for its part, may have the expertise, but it's stuck in the rut of only gathering and aggregating information on private sector cyber attacks. In the absence of enabling legislation the FBI have been meeting with big bankers urging them to report about attacks.

If the government is still at step one of cybersecurity--information sharing about attack--it appears that it cannot even manage that in a comprehensive way. On April 18, the House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA). It was dead on arrival in the Democratic Senate, due to White House opposition.

CBS News suggested the Administration opposed it "because language in its current draft suggests that companies like Facebook, Google and Twitter, share information with the federal government without a warrant." Huffington Post argued that the House bill doesn't "sufficiently protect privacy and civil liberties, ensure that a civilian department--not an intelligence agency--is the primary point of entry for cybersecurity information sharing, and provide narrowly tailored liability protections that would allow the private sector to respond to threats." And The Hill offered that "the final version of the bill did not satisfy the White House's key principles because it would allow companies to share cyber threat information directly with the military, including the National Security Agency (NSA), without being required to remove personal information from that data first." The Hill also said the current bill doesn't require companies to remove information on the identity of a specific person before sharing the threat information: "CISPA requires the government to strip that personal information from the cyber threat data it receives from companies instead."

A New bipartisan legislation [PDF], "The Deter Cyber Theft Act, S. 884" that was introduced on May 7th, by Sens. Carl Levin, D-Mich.; John McCain, R-Ariz.; Jay Rockefeller, D-W.Va.; and Tom Coburn, R-Okla.

Levin said we should hit those who commit cyberespionage in their wallets, "by blocking imports of products or from companies that benefit from this theft." The law would require an annual report listing the countries involved in cyberespionage and detail the kind of data the perpetrators were stealing. These lists could result in the president blocking imports of certain products from those countries. This would be a welcome step in the right direction.

The trouble is one cannot be sure how the White House would react. All of its actions regarding the Chinese cyberthreat have been "let's talk." While the administration has more than acknowledged China's depredations, no other steps seem to be taken. The Chairman of the Joint Chiefs of Staff, Gen. Martin Dempsey, recently visited with Chinese general Fang Fenghui, and talked about setting up a cybersecurity "mechanism." What does that mean? This seems to indicate that the administration is less interested in getting China to stop cyberattacks than it is in finding a compromise where no compromise ought to be seen as an outcome favorable to the United States. Remember: The Chinese want to regulate the Internet.

The May 6th Pentagon report openly blamed Chinese cyber attacks directly on its government and military. The report also said that Chinese espionage "was designed to benefit its defense and technology industry into U.S. policy makers' think about China." But there is nothing new in the report that we haven't known about for years. In fact latest reports say the Chinese have increased their cyberattacks.

If the Defense Department is so concerned about Chinese penetration of U.S. defense systems, as the report suggests, then how does it explain its recent $10.6 million contract with the Chinese for a year's use of their Apstar-7 satellite for data communications purposes?

On March 20, NASA administrator Charles Bolden told Congress that the agency "had closed down its technical reports database and imposed tighter restrictions on remote access to its computer systems" as a consequence of suspected espionage by an employee who happened to be a Chinese national. Bolden also said he had ordered to prevent access of "foreign nationals from designated countries -- including China, Iran and North Korea -- are given to NASA facilities and a moratorium on providing new access to citizens of those countries." Why do China, Iran, and North Korean nationals have access to NASA facilities, let alone serve as NASA contractors?

The Syrian Electronic Army's hacking of the AP Twitter account, and falsely

reporting on explosions at the White House, instantly wiped $136 billion off the DOW. The DOW came back. But what happened to those who lost the money?
A new venue for hacking into our financial system, the SEC trade-tracking computer system, has been recently introduced.
It is purportedly designed to insulate the market from flash crashes caused by High Frequency Trading and other glitches.

SEC Commissioner Mary Shapiro broke a 2-2 commission deadlock in favor of next-day reporting on hacking, instead of an immediate reporting ostensibly because the real-time version would be too costly.
Constantine von Hoffman has said, the market is now protected thus: "1) See horse in barn; 2) see horse leave barn; and 3) go close gate." Unfortunately, the same applies to the general state of U.S. cybersecurity.

FBI IC3 2012 Internet Crime Report

Source: http://www.stefanomele.it/news/dettaglio.asp?id=363

The FBI Internet Crime Complaint Center (IC3) has released the 2012 Internet Crime Report — a summary of reported fraudulent activity, including data and statistics.

In 2012, the IC3 received and processed 289,874 complaints, averaging more than 24,000 complaints per month. Unverified losses reported to IC3 rose 8.3 percent over the previous year.
A new section in this year's report includes charts for each of the 50 states detailing demographic, complaint, and dollar-loss data. The section allows for easy comparisons and convenient reference.
Additional content includes frequently reported Internet crimes, case highlights, and graphs that explain the lifecycle of a complaint. The most common complaints received in 2012 included FBI impersonation e-mail scams, various intimidation crimes, and scams that used computer "scareware" to extort money from Internet users.
The report gives detailed information about these and other commonly perpetrated scams in 2012.

► **Read the report here:** http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Police fear £2 app which lets mobiles use secret code could be used by terrorists to encrypt bomb plots

Source: http://www.dailymail.co.uk/news/article-2326768/2-app-lets-mobiles-use-secret-code-used-terrorists-bomb-plots.html?ito=feeds-newsxml

Venture capitalist Harvey Boulter, boss of Dubai-based developers behind the app said: 'If you're a law enforcement guy, you might have concerns'

Police and anti-terrorist agencies are facing a formidable new enemy – a cheap smartphone app that encrypts texts and phone calls, making them virtually impossible to bug.
Seecrypt, which costs £2 a month, allows users to apply a secret code to their messages and calls which gives them military-level security.
The system also makes it impossible for intelligence agencies to analyse which numbers terror suspects and criminals are calling, or when – a technique that is a mainstay of criminal investigation.
A senior UK official who has worked extensively in counter-

terrorism and against organised crime said he feared that Seecrypt would 'enable the bad guys to get ahead'.

Encrypted emails have been used by terrorists for years, he said, and sometimes proved impossible to crack.

'We're in a constant race against them and I suppose this is another issue we're going to have to deal with,' he said.

Porton Group, the Dubai-based investment fund behind the app, says it 'will work with law enforcement agencies to ensure this product does not fall into the wrong hands'.

But because the firm that will actually run the app is registered in the Cayman Islands, neither UK nor other Western security agencies will have any legal right to obtain warrants to gain 'real-time' access to unencrypted calls.

Former head of Defence Intelligence Staff Sir Joseph French said the app is 'at the top of the security ladder'

Seecrypt is extraordinarily easy to use. Subscribers are given a special, secret number prefixed by the code +281, and can then call or text anyone else with a Seecrypt account.

The app uses the internet to transmit the call, using either a wi-fi connection or an ordinary mobile phone signal. Calls to far-flung parts of the world are therefore free.

Seecrypt functions by generating a one-time cipher composed of two 'layers' of 2,048 digits every time subscribers contact each other.

Sources say it would take a super-computer at GCHQ – Britain's communications intelligence agency – about six months to break a code with just one layer of encryption at this level.

Seecrypt allows users to make and receive secure voice calls and text messages. Anti-terrorist agencies say this is an obstacle they will have to overcome

Sir Joseph French, a former head of the Defence Intelligence Staff, is one of Seecrypt's advisers.

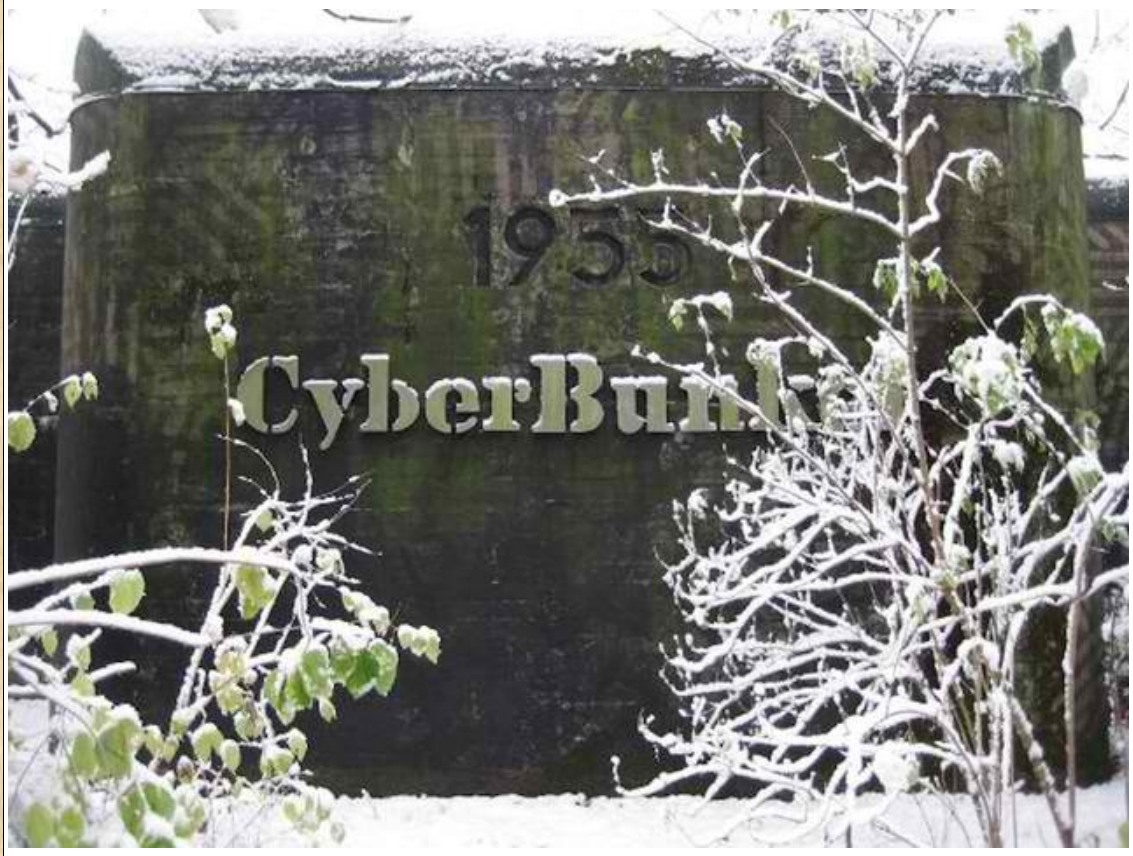
He said the app met the encryption standard required for official communications classified as 'Secret', and is 'at the top of the security ladder'.

Seecrypt is the direct descendant of Cellcrypt, Porton Group's military-grade app, which has been certified as virtually bug-proof by GCHQ. Cellcrypt is widely deployed by Coalition forces in Afghanistan as well as law enforcement and intelligence organisations around the world.
Porton's chief executive is Harvey Boulter, the businessman who first exposed the bizarre relationship

between former Defence Secretary Liam Fox and his bogus 'special adviser', Adam Werrity.
It was when the three men met in Dubai in 2011 to discuss the progress of Cellcrypt that Mr Werrity gave Mr Boulter a business card that falsely suggested he had a formal Ministry of Defence position.
In fact, although Mr Werrity had been best man at Dr Fox's wedding and travelled the world at his side, with his bills paid by a network of political donors, he had neither security clearance nor any official post.
The ensuing scandal forced Dr Fox to resign. He is currently suing Mr Boulter for libel over comments he made in a television interview.
Mr Boulter said Seecrypt expected to have a million subscribers within its first three months, and already had the capacity to go to 25 million.
He maintained it was aimed at 'anyone who wanted to restore their privacy', adding that the US had estimated that industrial espionage conducted against private business by China alone was costing the American economy about £750 billion a year.
A senior UK counter-terrorist official said that terrorists have been using encrypted emails for years, some which are impossible to crack
Mr Boulter admitted: 'If you're a law enforcement guy, you might have concerns. For them, it's not going to be entirely helpful.'
But he continued: 'People's privacy has been invaded more and more during the past decade. This will enable you to get some of it back.'
Also working on Seecrypt's development is Tony Chapa, the former chief technology officer of the US Secret Service – the body responsible for every aspect of the President's security.
He said: 'Your mobile phone is the open window on your privacy. Of course Seecrypt could be exploited by villains, but we will do everything we can to stop it being misused.'

'Largest' public denial of service attack in internet history linked to European spam dispute

Source: http://www.theverge.com/2013/3/27/4152540/largest-ddos-attack-spamhaus-linked-to-cyberbunker-spam



If your internet service has been running slower than usual lately, your cable company may not be the one to blame: a massive distributed denial of service (DDoS) attack that began on March 18 against the website of Spamhaus, a European volunteer spam-fighting organization, has increased to the point that it's now affecting websites around the globe, including Netflix, according to *The New York Times* and the BBC. Experts said it was the largest attack of its kind publicly identified, and Spamhaus told the BBC that law enforcement in five different countries were investigating the attacks.

The precise identity of the attackers remains unknown for now, but the *Times* and BBC quoted Sven Olaf Kamphuis as their spokesperson. Kamphuis said the attacks were being carried out in retaliation for Spamhaus's recent move to add a libertine Dutch domain hosting company named Cyberbunker to its list of suspected spam-hosting websites. Spamhaus recommends email operators block all traffic from the sites on this list, but Kamphuis accused Spamhaus of "abusing their influence." Cyberbunker maintains it doesn't host spammy domains.

It's not the first time that Spamhaus has been attacked, nor the first time it has accused Cyberbunker of hosting spammy domains. The feud between the two goes back to 2011, but this seems to be the first time it's spilled out onto the wider web in such a dramatic way.

For what it's worth, Cyberbunker, located in an actual Cold War-era nuclear bunker in the Netherlands, openly advertises that its "customers are allowed to host any content they like, except child porn and anything related to terrorism. Everything else is fine." It's also publicly clashed with local government officials and says it has "had several run-ins with the law," for protecting customer anonymity and data. Spamhaus, meanwhile, has been likened to an older "group of anti-spam vigilantes" that got "carried away" and added non-spam sites to its list, according to Y Combinator founder Paul Graham.

Whoever is behind the attacks on Spamhaus this time, they managed to set a record amount of traffic used to commit a DDoS attack, 300 gigabits per second, according to the *Times*. DDoS attacks work by

flooding websites with more traffic than they are equipped to handle, but most of these types of attacks are much smaller, around 10 gigabits per second. To mitigate this record attack, Spamhaus turned to security firm Cloudflare, who seems to have done the trick, as Spamhaus is now back online. It's unclear where the dispute between the two European web groups goes from here, but hopefully whatever happens next, they keep the rest of us out of it.

Cyber and Physical Security Special Report

Source:http://forms.erepublic.com/EM-Paper-step1-default?r=EM-Paper-step2-default&contentID=177907381

States and municipalities around the country are becoming inundated with security assaults. In an exclusive new survey conducted by the Center for Digital Government (CDG), senior IT and security department decision-makers report that 81 percent are bracing for cyber threats to rise over the next year, while 51 percent expect physical threats will also increase in the same period. It is now clear that defenses must grow in sophistication, and that security strategies require a higher level of coordination than ever between groups responsible for protecting IT resources and those working to keep intruders outside of protected facilities.

Fortunately, state and local security officials are far from facing these risks alone. Agencies of all sizes can draw on lessons learned — and shared — by their peers, along with a steady stream of commercial innovations from security solutions companies. This Special Report drills into these best practices, offers case study highlights of successful security policies across the country, reports additional details from the latest CDG research and provides a list of the top tools available today to defend against the shadowy community of domestic and international intruders.

Kaspersky Lab Uncovers 'Operation NetTraveler,' a Global Cyberespionage Campaign Targeting Government-Affiliated Organizations and Research Institutes

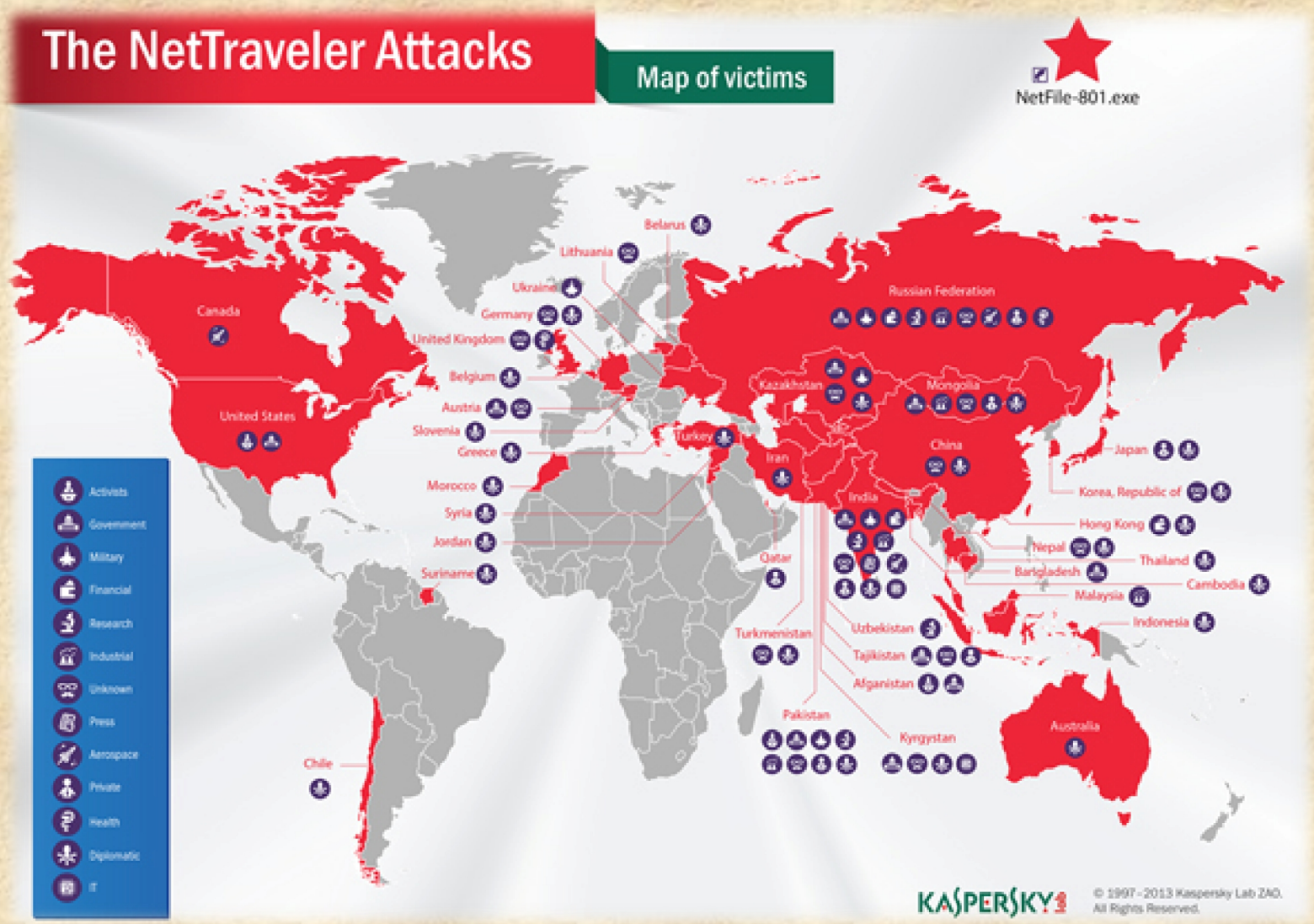
Source:http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Uncovers_Operation_NetTraveler_a_Global_Cyberespionage_Campaign_Targeting_Government_Affiliated_Organizations_and_Research_Institutes

Today (June 4th) Kaspersky Lab's team of experts published a new research report about NetTraveler, which is a family of malicious programs used by APT actors to successfully compromise more than 350 high-profile victims in 40 countries. The NetTraveler group has infected victims across multiple establishments in both the public and private sector including government institutions, embassies, the oil and gas industry, research centers, military contractors and activists.

According to Kaspersky Lab's report, this threat actor has been active since as early as 2004; however, the highest volume of activity occurred from 2010 – 2013. Most recently, the NetTraveler group's main domains of interest for cyberespionage activities include space exploration, nanotechnology, energy production, nuclear power, lasers, medicine and communications.

Infection Methods:

- Attackers infected victims by sending clever spear-phishing emails with malicious Microsoft Office attachments that are rigged with two highly exploited vulnerabilities (CVE-2012-0158 and CVE-2010-3333). Even though Microsoft already issued patches for these vulnerabilities they're still widely used for exploitation in targeted attacks and have proven to be effective.
- The titles of the malicious attachments in the spear-phishing emails depict the NetTraveler group's dogged effort of customizing their attacks in order to infect high-profile target. Notable



titles of malicious documents include:

- Army Cyber Security Policy 2013.doc
- Report - Asia Defense Spending Boom.doc
- Activity Details.doc
- His Holiness the Dalai Lama's visit to Switzerland day 4
- Freedom of Speech.doc

Data Theft & Exfiltration:

- During Kaspersky Lab's analysis, its team of experts obtained infection logs from several of NetTraveler's command and control servers (C&C). C&C servers are used to install additional malware on infected machines and exfiltrate stolen data. Kaspersky Lab's experts calculated the amount of stolen data stored on NetTraveler's C&C servers to be more than 22 gigabytes.

- Exfiltrated data from infected machines typically included file system listings, keyloggs, and various types of files including PDFs, excel sheets, word documents and files. In addition, the NetTraveler toolkit was able to install additional info-stealing malware as a backdoor, and it could be customized to steal other types of sensitive information such as configuration details for an application or computer-aided design files.

Global Infection Statistics:

- Based on Kaspersky Lab's analysis of NetTraveler's C&C data, there were a total of 350 victims in 40 countries across including the United States, Canada, United Kingdom, Russia, Chile, Morocco, Greece, Belgium, Austria, Ukraine, Lithuania, Belarus, Australia, Hong Kong, Japan, China, Mongolia, Iran, Turkey, India, Pakistan, South Korea, Thailand, Qatar, Kazakhstan, and Jordan.
- In conjunction with the C&C data analysis, Kaspersky Lab's experts used the Kaspersky Security Network (KSN) to identify additional infection statistics. The top ten countries with victims detected by KSN were Mongolia followed by Russia, India, Kazakhstan, Kyrgyzstan, China, Tajikistan, South Korea, Spain and Germany.

Additional Findings

- During Kaspersky Lab's analysis of NetTraveler, the company's experts identified six victims that had been infected by both NetTraveler and Red October, which was another cyberespionage operation analyzed by Kaspersky Lab in January 2013. Although no direct links between the NetTraveler attackers and the Red October threat actors were observed, the fact that specific victims were infected by both of these campaigns indicates that these high-profile victims are being targeted by multiple threat actors because their information is a valuable commodity to the attackers.

Obama orders U.S. intelligence to develop a list of targets for U.S. cyberattacks

Source: http://www.homelandsecuritynewswire.com/dr20130610-obama-orders-u-s-intelligence-to-develop-a-list-of-targets-for-u-s-cyberattacks

President Barack Obama has ordered U.S. intelligence agencies to develop a list of overseas targets for possible offensive cyberattacks by the United States.

The *Guardian* reports thatthe 18-page directive was issued last October. It says that "The secretary of defense, the DNI [Director of National Intelligence], and the director of the CIA … shall prepare for approval by the president through the National Security Advisor a plan that identifies potential systems, processes and infrastructure against which the United States should establish and maintain Offensive Cyber Effects Operations (OCEO) capabilities…."

The document says the government will "identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power."

The document defines OCEO as "operations and related programs or activities … conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks. "

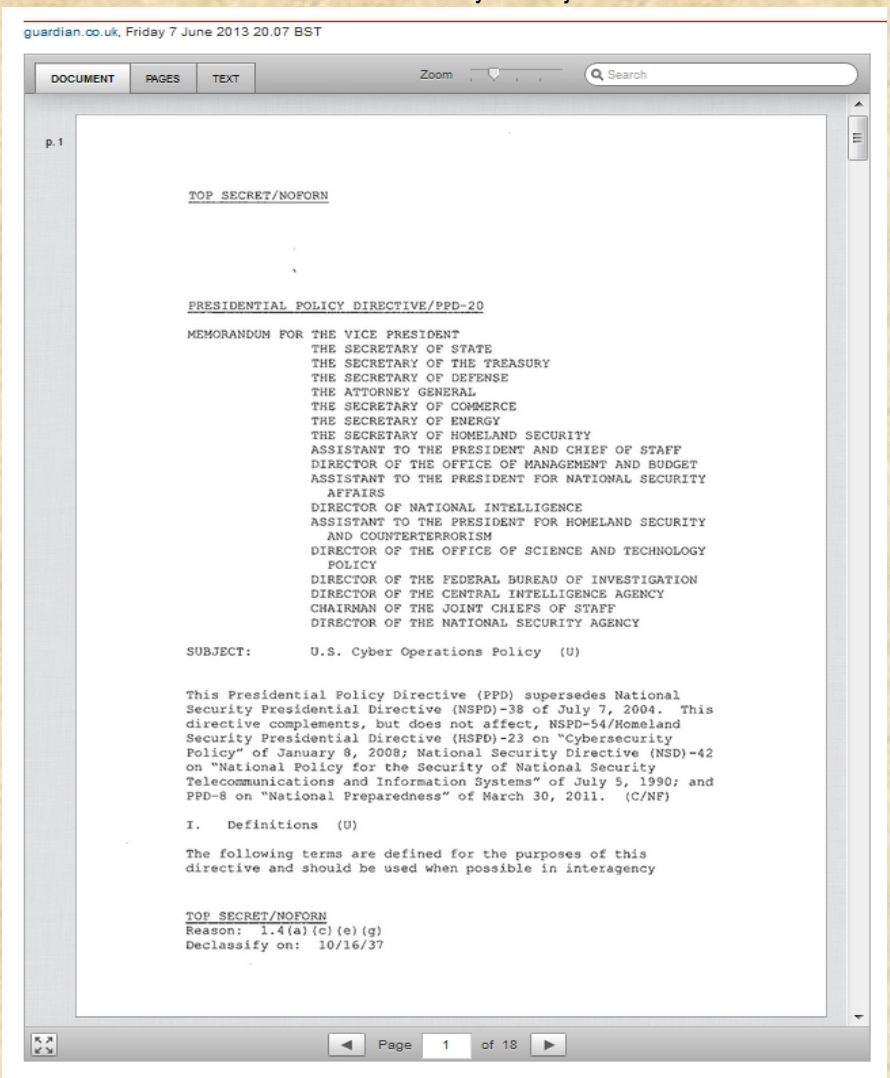
The document also says these operations "can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

The Guardian notes that parts of the directive have been gradually declassified, but the unclassified parts only involved intrusion detection systems for protecting federal computer networks, as well as discussing the government's role in securing critical infrastructure. The classified parts of the directive detail the U.S. plans to begin cyber offensive operations against foreign targets.

A senior official, who insisted on annonymity, told the *Guardian* that the plan is just the natural evolution of things.

"Once humans develop the capacity to build boats, we build navies. Once you build airplanes, we build air forces," he said.

The document does say that all U.S. cyber operations should comply with U.S. and international law and work only in conjunction with diplomatic and military operations. Presidential approval will be required for all actions which are "reasonably likely to result in significant consequences," meaning the loss of life, property damage, severe retaliation, or adverse foreign policy and economic impacts.



guardian.co.uk, Friday 7 June 2013 20.07 BST

DOCUMENT PAGES TEXT Zoom Search

p. 1

TOP SECRET/NOFORN

PRESIDENTIAL POLICY DIRECTIVE/PPD-20

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF ENERGY
THE SECRETARY OF HOMELAND SECURITY
ASSISTANT TO THE PRESIDENT AND CHIEF OF STAFF
DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
DIRECTOR OF NATIONAL INTELLIGENCE
ASSISTANT TO THE PRESIDENT FOR HOMELAND SECURITY AND COUNTERTERRORISM
DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
DIRECTOR OF THE NATIONAL SECURITY AGENCY

SUBJECT: U.S. Cyber Operations Policy (U)

This Presidential Policy Directive (PPD) supersedes National Security Presidential Directive (NSPD)-38 of July 7, 2004. This directive complements, but does not affect, NSPD-54/Homeland Security Presidential Directive (HSPD)-23 on "Cybersecurity Policy" of January 8, 2008; National Security Directive (NSD)-42 on "National Policy for the Security of National Security Telecommunications and Information Systems" of July 5, 1990; and PPD-8 on "National Preparedness" of March 30, 2011. (C/NF)

I. Definitions (U)

The following terms are defined for the purposes of this directive and should be used when possible in interagency

TOP SECRET/NOFORN
Reason: 1.4(a)(c)(e)(g)
Declassify on: 10/16/37

Page 1 of 18

Asked about the stepping up of U.S. offensive capabilities outlined in the directive, a senior administration official told the *Guardian*: "Once humans develop the capacity to build boats, we build navies. Once you build airplanes, we build air forces."

Caitlin Hayden, National Security Council spokeswoman, said in a statement:

> *We have not seen the document the Guardian has obtained, as they did not share it with us. However, as we have already publicly acknowledged, last year the president signed a classified presidential directive relating to cyber operations, updating a similar directive dating back to 2004. This step is part of the administration's focus on cybersecurity as a top priority. The cyber threat has evolved, and we have new experiences to take into account.*
>
> *This directive establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal. It provides a whole-of-government approach consistent with the values that we promote domestically and internationally as we have previously articulated in the International Strategy for Cyberspace.*
>
> *This directive will establish principles and processes that can enable more effective planning, development, and use of our capabilities. It enables us to be flexible, while also exercising restraint in dealing with the threats we face. It continues to be our policy that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as the preferred courses of action. The procedures outlined in this directive are consistent with the US Constitution, including the president's role as commander in chief, and other applicable law and policies."*

Israel accelerates cybersecurity know-how as early as 10th grade

By Christa Case Bryant

Source: http://www.csmonitor.com/World/Middle-East/2013/0609/Israel-accelerates-cybersecurity-know-how-as-early-as-10th-grade

With double the number of scientists and engineers per capita compared to the US and 10 times more active-duty soldiers relative to its total population, Israel already has impressive human capital in scientific fields such as cybersecurity. But now it is also tapping everything from high school classrooms to venture capital firms to extract cream-of-the-crop cyber experts, hone their skills and ideas, and fund their development.

Israel's model, though tailor-made for its unique size and capabilities, offers potential lessons for other countries looking to improve their cybersecurity game, including the United States, according to US cybersecurity experts familiar with Israel's approach.

The US has numerous programs in place to attract and train the best cyber talent, and President Obama recently proposed expanding the cybersecurity budget by nearly $1 billion after an annual US intelligence survey ranked the threat of cyberattacks on banks, power grids, and other infrastructure as higher than terrorism or weapons of mass destruction.

But quality can matter more than quantity in this emerging battlefield, where a team of pony-tailed hackers fueled by pizza, Coke, and plum salaries may be enough to design major attacks or help bolster US defenses against them.

Some American experts say Israel may be zeroed in to an even greater degree than the US on developing cyber Top Guns with the ability to write and modify computer code, spot software vulnerabilities, move clandestinely inside networks, and manipulate systems, rather than just develop cybersecurity policy.

"What Israel has done is focus much more heavily on technical skills and leave the political work to the politicians," says Alan Paller of the SANS Institute, who examined Israeli cybersecurity strategy as part of the US Department of Homeland Security's Task Force on CyberSkills last summer. "Their skill level [per capita] … outdoes everyone, even China," he adds, despite China's "massive program" for developing skilled cyber experts.

Professor Isaac Ben Israel, a driving force behind the creation of Israel's new National Cyber Bureau last year, says Israel has "the pleasure, the benefit, of selecting the right people for the right positions," thanks in large part to mandatory military service, which pools the country's talent and makes for efficient recruiting.

Such expertise helped Israel achieve a top-3 ranking in preparedness for cyberattacks in a 2012 report by security technology company McAfee, along with Finland and Sweden and ahead of the US, China, and Russia. In addition, Israel's critical infrastructure has been required by law to protect itself against cyberattacks since 2002, a decade before US Congress tried and failed to pass similar legislation. Israel has also implemented a host of new strategies in the past few years, including more math and science emphasis in schools, cybersecurity competitions, and major conferences such as Prof. Ben Israel's 3rd Annual International Cyber Security Conference that opens June 12 at Tel Aviv University with an all-star lineup of speakers, from Russia's Eugene Kaspersky to former White House official Richard A. Clarke.

Even so, Israeli experts remain concerned about enemies like Iran, which has the capacity to work on long-term attacks that require significant manpower, robust funding, and intelligence agents necessary to determine the location and type of computers used at, say, a power production company.

"In relative terms, we are in good shape," says Ben Israel, a former major general in the air force and one of Israel's most prominent cybersecurity experts. "In absolute terms, we are not in the required shape. Unfortunately we have more threats than Finland, Sweden, or even the United States."

New cyber incubator

One of the recommendations made by Ben Israel's task force was to further integrate academia, hi-tech industry, and the military. Together, all three fields create an ecosystem for

cultivating cyber talent, both in cyberwarfare and the growing commercial market for cybersecurity software.

Exhibit A of this ecosystem is the southern Israeli city of Beersheva. It is home to Ben Gurion University (BGU), which last year became the first Israeli university to offer a graduate track in cybersecurity, as well as a massive new military communications complex set to open in 2014, which will include the main cybersecurity training center for the Israel Defense Forces (IDF).

Adjacent to the IDF campus is the Advanced Technologies Park in Beersheva, a 2 million square-foot complex that is set to open its first building in July and is wooing multinational corporations with government incentives that include up to 10 years of tax exemption and salary subsidies of up to 50 percent. Among the outfits already committed to the park are Deutsche Telekom and EMC, whose RSA division is involved in cybersecurity, as well as a new cybersecurity incubator, JVP Cyber Labs.

Jerusalem Venture Partners (JVP), which was recently ranked as one of the world's 10 most successful venture capitalist firms, has among their holdings CyberArk, which began as a start-up with two graduates of the Israeli military's IT unit and today serves 7 of the 10 largest banks in the world. The founders' military service gave them, like many other former soldiers, a clear sense of where key security weaknesses lay.

"You can create great companies around that," says Gadi Tirosh, general partner at JVP. "So that's one area of talent that gives us in Israel a secret sauce to our Cyber Valley here in Israel."

JVP benefits from Israel's Chief Scientist Program, which contributes $500,000 for the first $100,000 investment JVP makes in its start-ups. "We can experiment with many more ideas at lower risk," says Mr. Tirosh, noting that JVP can conduct a $1 million "experiment" for half the cost.

The new JVP incubator in Beersheva is aiming to invest in four start-ups per year, with the first to be announced early in the fourth quarter of 2013.

"The Cyber Labs team is already active in identifying potential first investments, with key themes including zero-day attacks, advanced persistent threats, mobile security, and big data forensics," says JVP partner Yoav Tzruya, a former Air Force intelligence officer who is leading the incubator in cooperation with BGU.

JVP is benefiting from military-honed expertise not only in Mr. Tzruya but also venture partner Nimrod Kozlovsky, a former captain in the IDF's electronic warfare unit.

New cybersecurity grad program

Bracha Shapira, the head of BGU's Information Systems Engineering department, says the proximity of the new military campus and the new technology park with the JVP incubator will boost the university both financially and in terms of research opportunities.

"When you collaborate, industry gives you money to research," she says. "Also, you work on more interesting things because you understand the real problems that industry and defense [are facing] …. You get good sources of data, and really get to work on cutting-edge technology."

The government is also offering scholarships of up to 300,000 shekels ($83,000) as part of a 50 million shekel program to promote research on protecting Israel's networks and websites as well as exploring ethical and psychological questions related to cybersecurity.

Given the uptick of interest and funding in the field, Professor Shapira says she hopes to roughly double the number of students in the new cybersecurity graduate track from 16 this past year to 30.

Military hones program for high-school cyber geeks

The IDF sends select soldiers to universities such as BGU for specialized training, especially in the sciences. But given the urgent need for tale nt, the IDF launched a special program three years ago to identify exceptionally qualified high school students and begin their cybersecurity training as early as 10th grade. Currently 200 students are enrolled in the program, but graduates have so outperformed their peers in the IDF that commanders are clamoring for more. So this year the program will double in size, and the IDF hopes to see 1,000 students involved within two years.

"It costs money but they're willing to spend more money. If they're willing to pay you, it means you deliver," says Lt. Col. Sagi, who helps manage the *Magshimim* program, which is supported by the national cyber

bureau and the private Rashi Foundation as well as the IDF. "And we think we deliver very good students, or cyber experts."

The application process is highly competitive, and includes a two- to three-hour written test as well as a one-on-one interview. Each week, students meet six hours after school and do two to four hours of homework. They are taught by university students but the overall structure of the program is overseen by the IDF, which built it from scratch as no other similar models existed.

"We change it every year, because as you know when you build something from scratch you have a lot of changing and a lot of tuning to do," says Sagi. "I think it's getting better every year."

But so are Israel's cyber enemies.

Indeed, the number of cyberattacks on Israel is rising "exponentially," says Ben Israel. "We have to run very fast in order to stay in the same place. But we are doing it."

Christa Case Bryant is The Christian Science Monitor's Jerusalem bureau chief, providing coverage on Israel and the Palestinian territories as well as regional issues. She previously served as Middle East editor, coordinating the Monitor's network of correspondents from Tripoli to Tehran. She capped her 2009-12 tenure as a fellow on the International Reporting Project's Gatekeepers trip to Saudi Arabia. Prior to that she served as Europe editor, reporting from Berlin and Moscow. Ms. Bryant is a graduate of Principia College, where she focused on the Israeli-Palestinian conflict through her major in global perspectives and minor in religion. After many years as a cross-country ski racer on the national and international level, Ms. Bryant also has a special interest in all things Olympic, and covered the 2010 Vancouver Games for the Monitor.

QUIZ

How much do you know about cybersecurity?

Source: http://www.csmonitor.com/USA/2011/0420/How-much-do-you-know-about-cybersecurity-Take-our-quiz./william-gibson-neuromancer

Colleges expand programs as cybersecurity threats grow

Source: http://www.usatoday.com/story/news/nation/2013/06/03/cybersecurity-threats-grow-workers-needed/2386327/

Fueled by an increase in cyber attacks on critical infrastructure -- nearly 200 last year compared with fewer than a dozen in 2009, the federal Department of Homeland Security says -- cybersecurity has become among the hottest job markets in the country and an increasing focus of universities.

Farooq Alkhateeb of Independence, Ohio, just graduated from the University of Cincinnati, but he isn't terribly worried about finding a job as he majored in information technology and founded a campus group called Cybercrime Cats.

"There's so many opportunities, it's almost hard to sift through them all," he said.

While it's clearly become a cool major for students to consider, it also carries a dark side: Hackers launching attacks that can devastate the daily lives of citizens and put businesses into panic as their most basic systems are infected.

Online attacks can disrupt banking, health care or even electronic identities, as well as infrastructure such as utilities or financial markets that could disrupt daily lives for millions of people.

Analysts earn median pay of about $75,000 a year and more than 65,000 new jobs will be created by 2020, the U.S. Labor Department says.

Those workers are desperately needed, experts said, because the quest for information online is multiplying just as the need for security becomes more critical.

"This isn't a fad," said University of Cincinnati political science professor Richard Harknett, a member of Ohio's Cyber Security Education and Economic Development Council. "We keep doubling down on this. We're doubling down on an insecure infrastructure for convenience and efficiency."

Whether the motive is money, strategic advantage or simply to wreak havoc, the attacks have gotten more serious and more brazen during the last few years.

The Obama administration recently accused China of mounting a series of cyber attacks on government or military targets.

And in May, prosecutors in New York arrested several people after hackers managed to steal $45 million by illegally tapping into automated teller machines more than 40,000 times.

Attacks can range from using infected attachments to hack into personal e-mails, to sophisticated schemes that use one computer as a launching pad that can tap into large data storehouses.

For every confirmed attack, there are thousands of attempts.

For example, utilities across the country have reported nearly constant attacks. According to a congressional report last year, one utility reported it was the target of 10,000 attempted attacks each month.

Last year, the Department of Homeland Security processed about 190,000 "cyber incidents" against critical infrastructure or federal agencies, up 68% from the year before.

The stakes are immense.

"Our daily life, economic vitality and national security depend on cyberspace," top Homeland Security officials said in written testimony to Congress in May. "A vast array of interdependent IT networks, systems, services, and resources are critical to communicating, traveling, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks."

'It's kind of scary how simple it is.'

With the problem growing, universities are stepping up academic programs to provide the workers they will need.

Nearly every university teaches computer science and information technology courses. The newest trend is packaging those courses into certificates and degree programs aimed at supplying workers to a far-flung network of cybersecurity employers.

For example, Northern Kentucky University will debut its data science major this fall and a group of students on a cyber defense team have shown success in national competitions.

Yi Hu, the Northern Kentucky University computer science professor who coaches the team, said students learn the importance of maintaining customer service even in the face of a behind-the-scenes attack.

"Not only do students need to have a skill to defend their systems, they need to have the skills to fight back," he said.

Starting this fall, the University of Cincinnati will offer a cybersecurity certificate including classes from political science, criminal justice and information technology.

In a class this spring, Harknett and colleague Mark Stockman set up scenarios for their students, including one in which a group including Alkhateeb modeled an "attack" on a bank in the Middle East, reading actual code that showed exploitable flaws in the bank's Web pages to steal credit card numbers.

"We said, 'This area of the world is growing so fast that they're probably not worrying too much about security,' " Alkhateeb said. "It's kind of scary how simple it is."

In that case, the attackers' motive was stealing millions of dollars, but the design of any attack often is not that simple.

Overall, Alkhateeb said, anyone with basic knowledge of coding and IT infrastructure can launch attacks.

"If anybody tells you it can be 100% foolproof, no," he said.

Potential jobs are only one reason programs teaching cybersecurity are so popular with students.

"Hackers are becoming like the cool thing now," he said. "But your goal should be learning what the hackers are doing and how to defend against it. That's even more fun."

How to protect yourself from cyber attacks

• Never click on links in e-mails. If you think it is legitimate, go the site and log on directly.
• Never open the attachments from a retailer or other company.
• Do not give out personal information.
• Set secure passwords, avoid using common words or phrases, and update regularly.
• Keep your operating system and browser up to date.
• Verify authenticity of requests from companies. Contact them directly.
• Pay close attention to URLs. Malicious sites sometimes use a variation of a common spelling.
Source: U.S. Department of Homeland Security

Top 'threat actions' by cyber attackers

• Exploitation of default or guessable passwords, usually through remote Internet access -- 72%
• Backdoor attacks -- 49%
• Exploitation of command and control channel -- 49%
• Unknown -- 43%
• Repeating a "dictionary" of possible names and passwords.
Source: Verizon study of health care industry

Common methods used by hackers

✓ **Trojan Horse programs**: Tricks users into installing back-door programs allowing access to their computer.
✓ **Denial of service:** Causes a computer to crash.
✓ **Distributed denial of service:** Uses compromised computers as launching pad to attack other systems.
✓ **Mobile code:** Intruders can change codes such as Java to gather information.
✓ **Packet sniffing:** A program to capture data from "packets" of information traveling over the Internet.
Source: www.armor2net.com

Job market for cybersecurity

Graduates can become information security analysts, Web developers or computer network architects
2010 median pay: $75,660 per year
New jobs to be created, 2010-20: 65,700
Anticipated job growth, 2010-20: 22%

Source: U.S. Labor Department