Syrian CWAs – Are they under control?

Volume 45, 2012

CBRNE Newsletter Terrorism

Cyber News

www.cbrne-terrorism-newsletter.com

Power grid vulnerable to 'fast-moving cybersecurity threats'

By Declan McCullagh

Source: http://news.cnet.com/8301-1009_3-57501660-83/feds-power-grid-vulnerable-to-fast-moving-cybersecurity-threats/

Federal regulators charged with overseeing the reliability of the electrical grid expressed concerns about proposed cybersecurity standards and warned that existing law may not protect "against fast-moving cybersecurity threats."

Yesterday's statement from the Federal Energy Regulatory Commission came in a response to pointed questions from two senators, Joseph Lieberman (I-CT), the chairman of the Senate Homeland Security Committee, and Susan Collins (R-ME), the panel's senior Republican. The senators made their inquiries in July, a few weeks after CNET published an article on the topic.

Lieberman and Collins had asked for an "expeditious comprehensive investigation" into allegations that industry standards for digital signatures -- used for authentication, including access to control systems -- were insufficient.

FERC said that the industry's plans to allow 20-year expiration on digital certificates, even though shorter periods are more secure, is worrisome. "The commission is concerned that this time period may present an unacceptable risk of compromise... Such long life spans increase the likelihood of a user's keys or certificates being compromised," it said.

Complicating the situation is that FERC has deferred to an industry standards-setting body, called the North American Energy Standards Board, to act in this area. Although the board is a private organization, FERC has routinely adopted its standards as regulations, giving them the force of law, including the board's 2008 digital signature policy.

Because the standards board is revising its digital certificate standards, "further action by the commission does not appear necessary at this time," FERC concluded. It also said that the "commission does not have jurisdiction" over either the standards board or the certification authorities that issue keys used in digital signatures.

Digital certificates are documents that use a cryptographic signature for authentication, which can in turn be used to prove that a person is who he claims to be, or that computer code is trusted and can be executed. The Stuxnet malware used valid digital signatures issued by reputable

companies to bypass anti-virus applications and attack Iran's nuclear facilities. (Because even carefully designed algorithms may have flaws that will be discovered over time, as happened with the MD5 algorithm in 1995 and the SHA-1 algorithm in 2005, certificates are generally more secure if they expire more quickly, forcing updates.)

FERC added that its current authority "to enforce compliance with those standards is not adequate to address imminent cyber or other national security threats to the reliability of our transmission and power system," but declined to endorse any specific legislation.

Nevertheless, that could give a boost to Lieberman's bill, which would give the U.S. government additional authority to regulate cybersecurity practices for critical infrastructure, or related legislation such as the so-called GRID Act.

Lieberman's Cybersecurity Act of 2012 was blocked by Republicans earlier this month; they favor a competing GOP-backed measure.

Jesse Hurley, co-chair of the North American Energy Standards Board's Critical Infrastructure Committee, told CNET in June that the mechanism for creating digital signatures is insufficiently secure because not enough is being done to verify identities.

While FERC agreed with him that 20-year expirations are too long, it concluded that Hurley did not "provide specific evidence to support the allegations" about poor identity verification. He told CNET this morning that "it's clear that (FERC is) trying to punt to Congress and bolster their request for more authority."

Two companies, Open Access Technology International (OATI) and GlobalSign, which are authorized by the NAESB to issue digital certificates to the industry, argue that a 30-year expiration for digital certificates is fine.

"OATI doesn't see a problem with 30 years from a security standpoint," Patrick Tronnier, OATI's principal security architect, said on a NAESB conference call on May 31. Tronnier responded to complaints about weakened security by saying it would cause too much "disruption" to choose a shorter period.

***Declan McCullagh** is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.*

Facespook: Russian spies order $1mln software to influence social networks

Source: http://rt.com/politics/intelligence-orders-influencing-social-619/

Russia's Foreign Intelligence Service (SVR) has ordered three systems worth about US$1 million that will automatically spread information on the Internet.

The systems were ordered in a three separate tenders and the official client's name is Military Unit 54939, but Kommersant Daily newspaper, which broke the news, writes that according to its sources this military unit belongs to the Foreign Intelligence Service's structure.

The first system is called Dispute and is responsible for overall monitoring of the blogosphere and social networks in order to single out the centers where the information is created and the ways by which it is spread among the virtual society. It also looks at factors that affect the popularity of various reports among internet users.
The second system, Monitor-3, will develop the methods of organization and management of a "virtual community of attracted experts" – setting of tasks, control over work and regular reports on chosen issues.
The third, and probably most important, of the systems is Storm-12 – its task is to automatically spread the necessary information through the blogosphere, as well as "information support of operations with pre-prepared scenarios of influence on mass audience in social networks."
The first two systems are to be ready by the end of 2012 and the third by 2013.
According to Kommersant, all three tenders were won by the company Iteranet, headed by a former deputy head of the Russian Cryptography Institute, Igor Matskevich, who previously worked on top secret state orders.
The newspaper claims that the tenders were held in a top secret mode and does not specify how the information was obtained or the reasons for deciding to disclose it.
Experts were cautious in their assessments of the new initiative. Russia's leading startup manager of internet projects Anton Nossik said that imbedded spam filters will resist the automated opinion-making systems and suggested that part of the budget must be spent on means to overcome this.
Another expert who preferred not to be named told Kommersant that the system can only be effective if its activities go beyond the legal sphere – like hacking the administrators' rights on social networks, mass messaging or even infecting the users' computers with automatic "bot" programs.
The head of the Russian association Center for Safe Internet, Urvan Parfentyev, said that the news was a natural development of conventional propaganda means, like the Voice of America and RFE RL radio stations, only on the internet.

Taliban Using Fake Facebook Accounts for Intelligence Gathering, Report Says

Source: http://mashable.com/2012/09/11/taliban-fake-facebook-intelligence/

An Australian government review of social media and defense, completed in March, revealed that the Taliban is using fake Facebook profiles to obtain intelligence from unsuspecting military personnel.

According to the report, one strategy employed by the terrorist organization is to pose as "attractive women" and friend deployed soldiers. Once friended, Taliban members can track the whereabouts of those soldiers thanks to Facebook's geo-tagging features.
"Most did not recognise that people using fake profiles perhaps masquerading as school friends, could capture information and movements," the report states. "Few consider the possibilities of data mining and how patterns of behaviour can be identified over time."
The review also claims that family and friends can put military missions at risk by sharing confidential data via social media.

A high percentage of those surveyed admitted that they weren't aware of the dangers that come with over-sharing via social media. 58% of the 1577 who participated in the review expressed that they were never properly trained to safely use social media.
Australia's Department of Defense said that its currently working on putting together a social media guide for soldiers heading into combat. However, these new guidelines will not be ready until Christmas 2012. The review recommends that soldiers do not share personal data like name, rank, and location via any social media platform.
The enemy using information obtained from social media is not entirely new. Earlier this year, the U.S. Army acknowledged that a 2007 attack that destroyed 4 U.S. Apache helicopters in Iraq was made possible by location data in photos shared by soldiers.

Spies and professors band together for UK cybersecurity research institute

Source: http://www.zdnet.com/uk/spies-and-professors-band-together-for-uk-cybersecurity-research-institute-7000004210/

The UK is to get an academic institute for researching the 'science of cybersecurity', the government and spy chiefs announced on Thursday.
The Research Institute in the Science of Cyber Security will open at the start of October and operate for the next three and a half years. It will be hosted at **University College London (UCL)**, funded through a £3.8m government grant and led by UCL professor Angela Sasse.
The Research Institute in the Science of Cyber Security will be based at UCL. Image: UCL

The institute is backed by the government, GCHQ, various research councils and seven universities, and is intended to get "social scientists, mathematicians and computer scientists from across the UK" working together.
"The UK is one of the most secure places in the world to do business — already eight percent of our GDP is generated from the cyber-world and that trend is set to grow," cybersecurity minister Francis

Maude said in a statement. "But we are not complacent. Through the National Cyber Security Programme we are putting serious investment into the best UK expertise to lead thought in the science of [cybersecurity]."
According to GCHQ, the objectives of the institute will include combating cyber-crime, making the UK more resilient against cyberattack and "better able to protect our interests in cyberspace", and to "help to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies".

Cybersecurity efforts

The news of the institute came a day after the European Commission said its Computer Emergency Response Team (CERT), which has been piloted over the last year, would now be permanently established.
Digital agenda commissioner Neelie Kroes said in a statement that EU institutions could "now count on a permanent CERT to deal with increasingly sophisticated cyber-threats against them", and that the move "ensures we are practising what we preach".
Part of the remit of CERTs — both at the European and national level — is to give advice to public-sector organisations in particular about defending themselves against cyberattacks.
As for businesses, GCHQ said on 5 September that it had started advising "the UK's most senior business leaders" on dealing with internet-related threats. At the time, business secretary Vince Cable said companies should shore up their defences to protect their bottom line.
"Ensuring this happens should be the responsibility of any chief executive or chair as part of an approach to good corporate governance which secures a business for the long term," Cable said.

India ties up with US for cyber security

Source: http://www.dnaindia.com/india/report_india-ties-up-with-us-for-cyber-security_1740178

Waking up to the dangers of cyber attacks on its vital installations and government sites that have seen a spiralling increase in the past few years, India is entering into a collaboration with the US to learn how to develop a robust cyber security mechanism to safeguard its key and critical infrastructure areas.
To begin with, the Indian Computer Emergency Response Team's (Cert-In) two-day joint exercise with its US counterpart got underway on Wednesday. The two agencies will launch full-scale cyber attacks like phishing, network-probing, spread of malicious code like virus, worms and spam against each other in the virtual world and would also apply all defence mechanism at their command to thwart those attacks.
Afterwards, both agencies will analyse each others' areas of vulnerability in detail and suggest possible safeguards and would even workout fresh security programmes.
"It is not a secret that we are vulnerable to cyber attacks that are coming in increasing numbers from China and Pakistan besides some private hackers. We are hoping to learn a lot from the US, which perhaps has developed the most advanced robust cyber security mechanism. This will help us develop a cyber security infrastructure about which prime minister Manmohan Singh spoke at the police chiefs' conference," a senior official said.
The cyber security collaboration is an offshoot of the idea that was first mooted in the talks between Union home secretary RK Singh and deputy secretary of the US department of homeland security, Jane Lute in April.
"We have been seeking help from various countries in cyber security but this is for the first time that a joint exercise is being held under a long-term collaboration programme. India is also constituting a new cyber security architecture under the NSA," former Union home secretary GK Pillai told DNA.
Cyber security experts in the government concede India's weakness in countering cyber attacks from neighbouring countries and handling of powerful malwares like Flame and Stuxnet.
In a report to Parliament in May, CERT-In observed that there was significant increase in the number of cyber security attacks on vital installations and key government ministries like PMO and Union home ministry. A total of 8,266, 10,315 and 13,301 security incidents were reported to and handled by Cert-In during

2009, 2010 and 2011, respectively.

According to data compiled by the home ministry, 1,791 cases were registered under the Information Technology (IT) Act in 2011 against 966 in 2010 — an increase of over 85%. Cyber cases under the Indian Penal Code went up by 18.5% in 2011.

U.K.'s first research institute to investigate the science of cyber security

Source:http://www.homelandsecuritynewswire.com/dr20120916-u-k-s-first-research-institute-to-investigate-the-science-of-cyber-security

A new academic research institute, aiming to improve understanding of the science behind the growing cybersecurity threat, was announced last week.

GCHQ, the U.K. intelligence agency, says that the institute, which is funded by a £3.8 million grant, is part of a cross-government commitment to increasing the U.K. academic capability in all fields of cybersecurity. The institute's research will ultimately make it easier for businesses, individuals, and government to take informed decisions about how to implement better cyber protection measures and benefit, safely, from the opportunities offered in cyberspace.

Established by GCHQ, in partnership with the Research Councils' Global Uncertainties Program (RCUK), which is led by the Engineering and Physical Sciences Research Council (EPSRC), and the Department for Business Innovation and Skills (BIS), the Research Institute is a virtual organization involving seven universities. It will allow leading academics in the field of cybersecurity, including social scientists, mathematicians, and computer scientists from across the United Kingdom, to work together.

GCHQ says the institute will also connect them with the collective expertise of industry security experts and international researchers in the field to tackle some of the U.K.'s toughest challenges in cybersecurity, in both the public and private sectors.

This collaborative approach among academia, industry, and government will ensure that research is relevant and inspired by real world, cutting edge, security issues.

Francis Maude, Minister for Cyber Security, said:

> *The UK is one of the most secure places in the world to do business — already 8 percent of our GDP is generated from the cyber world and that trend is set to grow. But we are not complacent. Through the National Cyber Security Program we are putting serious investment into the best U.K. expertise to lead thought in the science of cyber. The U.K.'s first academic Research Institute will strengthen capability in a strategically important area, keeping the U.K. at the forefront of international research in the field.*

David Willetts, Minister for Universities and Science, said:

> *Britain has one of the largest online economies in the world and a growing cyber security sector, and we need to ensure this success continues. This new Research Institute will draw on the leading expertise in our universities from both technological and behavioral disciplines to address key challenges. It will help businesses, government and individuals to better protect themselves from cyber threats so they can make the most of the opportunities the internet presents.*

Universities were selected following a tough competitive process, in which they had to devise new research programs to address one of two key challenges:

- How secure is my organization?
- How do we make better security decisions?

Addressing these practical challenges requires a blended approach from researchers, drawing from both technological and behavioral disciplines. Four teams were successful:

- University College London, working with University of Aberdeen
- Imperial College, working with Queen Mary College and Royal Holloway, University of London
- Royal Holloway, University of London
- Newcastle University, working with Northumbria University.

University College London was selected to host the Research Institute, with Professor Angela Sasse taking the role of director of research.

The Research Institute will open for business on 1 October 2012 for a period of three-and-a-half years. Sasse said:

> *I am delighted to be leading the new research Institute. This is an opportunity to work closely with colleagues from different scientific disciplines to tackle the technical, social and psychological challenges that effective cyber security presents.*

The establishment of the Research Institute is part of the U.K. government's National Cyber Security Strategy. The strategy describes how government is working with academia and industry to make the United Kingdom more resilient to cyber attacks. The objectives of the strategy are to:

- Tackle cyber crime and make the United Kingdom one of the most secure places in the world to do business in cyberspace
- Make the United Kingdom more resilient to cyber attack and better able to protect our interests in cyberspace
- Help to shape an open, vibrant, and stable cyberspace which the U.K. public can use safely and that supports open societies
- Build the U.K.'s cross-cutting knowledge, skills, and capability to underpin all cyber security objectives.

Earlier this year, GCHQ, BIS, and RCUK announced the award of Academic Centre of Excellence (ACE) in Cyber Security Research status to eight U.K. universities.

GCHQ says that also in the pipeline are plans for a second Research Institute, increased sponsorship of Ph.D. research, and a scheme to recognize Academic Centers of Excellence in Cyber Security Education.

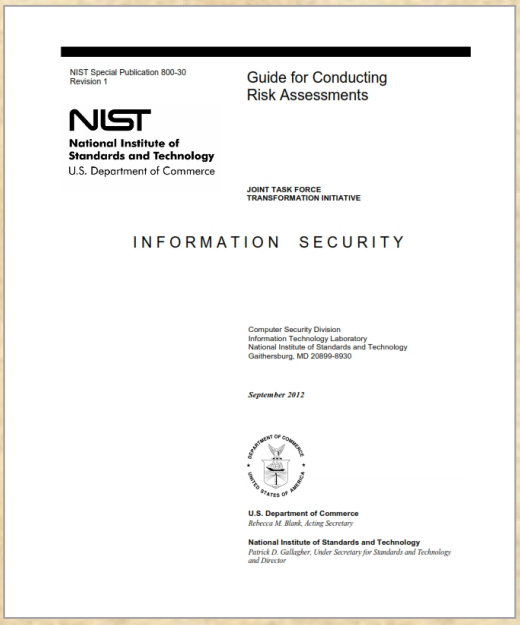
The organizations involved note that both the ACE and the Research Institute initiatives are harnessing the vital role that academia has to play in supporting the U.K.'s cybersecurity, but the roles are different. The ACE initiative recognizes existing areas of strength. The Research Institutes, on the other hand, are targeted investment to develop capability on strategically important topics.

The award of research grants to the universities in the Research Institute is subject to the universities agreeing to the GCHQ and RCUK terms and conditions.

In other areas, GCHQ, BIS, and RCUK are working together to advance the level of cyber education at all levels from GCSE through to post graduate research.

New NIST publication provides guidance for computer security risk assessments

Source:http://www.homelandsecuritynewswire.com/dr20120920-new-nist-publication-provides-guidance-for-computer-security-risk-assessments


NIST Special Publication 800-30
Revision 1

Guide for Conducting
Risk Assessments

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2012

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

The National Institute of Standards and Technology (NIST) has released a final version of its risk assessment guidelines which, NIST says, can provide senior leaders and executives with the information they need to understand and make decisions about their organization's current information security risks and information technology infrastructures.

"Risk assessments are an important tool for managers," explains Ron Ross, NIST fellow and one of the authors of Guide for Conducting Risk Assessments. "With the increasing breadth and depth of cyber attacks on federal information systems and the U.S. critical infrastructure, risk assessments provide important information to guide and inform the selection of appropriate defensive measures

so organizations can respond effectively to cyber-related risks."

A NIST release notes that information technology risks include risk to the organization's operations (including, for example, missions and reputation), its critical assets such as data and physical property, and individuals who are part of or served by the organization. In some cases, these risks extend to the nation as a whole. Risk assessments are part of an organization's total risk management process.

In March 2011, NIST released Managing Information Security Risk: Organization, Missions and Information System View (NIST Special Publication 800-39), which describes the process for managing information security risk for federal agencies and contractors. That process includes framing risk, assessing risk, responding to risk and monitoring risk over time.

The new publication, Guide for Conducting Risk Assessments, focuses exclusively on risk assessment — the second step in the information security risk management process. The guidance covers the four elements of a classic risk assessment: threats, vulnerabilities, impact to missions and business operations, and the likelihood of threat exploitation of vulnerabilities in information systems and their physical environment to cause harm or adverse consequences.

"As the size and complexity of our collective IT infrastructure grows, we cannot protect everything we own or manage to the highest degree," says Ross. "Risk assessments show us where we are most at risk. It provides a way to decide where managers should focus their attention."

The risk assessment guidance is designed to meet the needs of a variety of organizations, large and small, including financial institutions, health care providers, software developers, manufacturing companies, military planners and operators, and law enforcement groups.

The Guide for Conducting Risk Assessments (SP 800-30, Revision 1) completes the original series of five key computer security documents envisioned by the Joint Task Force — a partnership of NIST, the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Systems—to create a unified information security framework for the federal government. SP 800-39 is also in this series.

► The guide is available here. SP 800-39 is available here.

Canada needs to take threat of Chinese cyberespionage more seriously: former top spy

Colin Freeze (The Globe and Mail)
Source:http://www.theglobeandmail.com/news/politics/canada-needs-to-take-threat-of-chinese-cyber espionage-more-seriously-former-top-spy/article4598561/

One of Canada's former top spies says that the damage done by economic espionage is now on par with the threat posed by al-Qaeda and other radical groups.

"It has become equal to the threat of terrorism. Why? It has such long-term repercussions. The future prosperity of Canadians," says Ray Boisvert, who had served as the assistant director of intelligence for the Canadian Security Intelligence Service until his retirement six months ago.

Mr. Boisvert made his remarks to The Globe and Mail after Washington released a scathing report about the cyberespionage threat posed by China's Huawei Technologies Co.

The expanding telcom giant simply "cannot be trusted to be free of foreign state influence," according to the U.S. House Permanent Select Committee on Intelligence.

The report suggested Huawei and the billions of dollars worth of Internet-infrastructure equipment that it sells could facilitate "the ongoing onslaught of sophisticated computer network intrusions that originate in China."

Citing classified and unclassified intelligence, the lawmakers – versed in Washington's own clandestine hacking efforts – recommended that Huawei be kept far away from contracts to install sensitive U.S. government systems. Their fear? Chinese spies could prevail on Huawei to install backdoors that would allow for sneak peeks at propriety data – or worse, allow them to mess with U.S. infrastructure.

Huawei remains opaque about its ongoing ties to the one-party Communist state that nurtured it. So much so that the House intelligence committee is also telling private companies to give Huawei a wide berth.

The multibillion-dollar company counters that American fears are based purely on rumour and innuendo. Yet Australia and Great Britain, too, have also taken precautions to ensure their own networks are free of prying eyes where Huawei equipment is involved.

Such arrangements now threaten to leave Canada as the odd man out in the decades-old intelligence fraternity of major English-speaking powers – the only partner that hasn't yet publicly grappled with the significance of selling its data pipelines to a multinational often seen to be aligned with a rival power.

How significant is this Huawei issue from Canada? Here, Mr. Boisvert, who left CSIS to start a risk-management consultancy known as I-Sec Integrated Strategies, reflects on how Ottawa has been grappling with the issue.

The Globe and Mail: The U.S. seems to be very proactive about the Huawei issue.

Ray Boisvert: In this country, it's a lot more about doing business – Canada is a trading nation, we're small, and we need to take greater risks.

When it comes down to the U.S. polity versus ours, there's a lot more weight placed on security requirements.

There's a made-in-U.S.A. factor, too, that can't be ignored. In the U.S., there are a lot of telecommunications suppliers that could supplant Huawei's deliverables.

Well, we used to have a pretty good telecom equipment company in Canada. A lot of people suggest Huawei ate – or stole – Nortel's lunch ...

There was a bunch of stuff going on – a bunch of poor decisions were made. The Year 2000 high-tech collapse that played against Nortel.

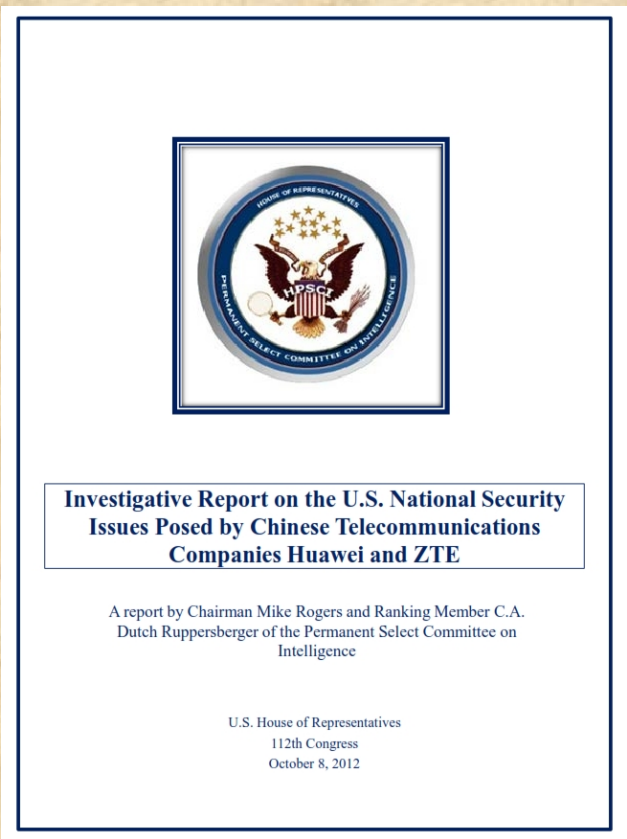
But there have been enough stories including the head of IT [information technology] at Nortel who said that "We got done by cyber-attacks."

And at the same time Huawei rose, Nortel fell. Coincidence? I don't think so.

How well equipped is the Canadian government to address espionage?

At the end of the day, we've all been focused on the post-9/11 environment. The single most important threat has been the threat of terrorism.

That has distracted us from a very important national security threat that all of us in the business are very conscious of.



Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE

A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence

U.S. House of Representatives
112th Congress
October 8, 2012

Espionage in the 21st Century is not spy-versus-spy but it's really about gaining strategic economic advantage, globally. That means agencies facilitating the companies to gain strategic advantage to dominate economically.
In my view, it has become equal to the threat of terrorism. Why? It has such long term repercussions. The future prosperity of Canadians.

What should Canadian lawmakers think about U.S. counterparts sounding the alarm about Huawei?
It comes down to: Is our policy attuned at the right level?
There's a two-part decision. One – Huawei, do you accept them as a legitimate player in the marketplace? If the answer to that is yes, then you are really hard-pressed not to allow them to compete for contracts in the private sector.
The second part is, are they a security threat? If they are should they be able to bid on shared [critical government] infrastructure?
It's one thing to lay down the backbone of a really large set of pipes. If you had some malware embedded in the coding of the system, you're fishing in a pond that's billions and billions of litres deep.
Versus, if you're sitting on a specific network where right away the fishing is pretty clear – you're in a small pond of a hundred litres. It's easier to identify which one of those data packages, which fish you want to spear.

But aren't people getting a lot better at sifting the important stuff out of torrents and torrents of data?
There are limits.
If you're asking me "Would you let them install hardware into the main telecommunications networks?," my answer would be "Yeah you could, but you really want to put in a lot of checks and balances – initial verification of the code, and ongoing auditing of all of the mechanisms that Huawei would implement."
Does this inform the Nexen Inc. takeover debate? Or are oil and telecom two different kettles of fish?
It's not the same national-security concern. It's one thing to look at the fact that here's a huge investment in a strategic resource – oil – and ask "Is this in Canada's best interest?"
But the Huawei one is very greatly debated. I think there is a preponderance of legitimate evidence, there is enough layman and specialist understanding, that an organization like Huawei could take incredible advantage of owning the network that all of your communications are crossing.

Have the security implications of Huawei been discussed in places like the Langevin Block? 24 Sussex? Your old shop at Blair and Ogilvie?
I'll just say that I know, when I was at CSIS, these issues were raised. Whether they have an audience or not, I'll leave that for others to comment on.
Canada has taken a look at those issues when the larger telecommunications companies [Telus, Bell, Rogers] wanted to buy Huawei equipment.
The role of CSIS is to give advice to Industry Canada.
So Industry Canada plays the middle man role – in terms of responding to concerns that industry may have [to government] or bringing those concerns the security community may have to industry.

Isn't there always a tension between the security guys and the "Do Business" guys? Does it make any sense to put the

cybersecurity issue within the "Do Business" Ministry?

There is certainly a tension. It's a tension that an organization like CSIS is fully aware of.

Iran may hit U.S. with first cyberattack

Source:http://www.washingtontimes.com/news/2012/oct/17/iran-may-hit-us-with-first-cyberattack/#ixzz29fdiEe00

Defense Secretary Leon E. Panetta's pointed warning that the United States will strike back against a cyberattack underscores the Obama administration's rising concern that Iran could be the first country to unleash cyberterrorism on America.

Mr. Panetta's unusually strong comments last week came as former U.S. government officials and cybersecurity experts said the United States thinks Iranian-based hackers were responsible for cyberattacks that devastated computer systems of Persian Gulf oil and gas companies.

Unencumbered by diplomatic or economic ties that restrain other nations from direct conflict with the United States, Iran is an unpredictable foe that national security experts contend is not only capable but willing to use a sophisticated computer-based attack.

Mr. Panetta made it clear that the military is ready to retaliate — though he didn't say how — if Washington believes the nation is threatened by a cyberattack, and he made it evident that the United States would consider a pre-emptive strike.

"Iran is a country for whom terror has simply been another tool in their foreign policy toolbox, and they are a country that feels it has less and less to lose by breaking the norms of the rest of the world," said Stewart Baker, former assistant secretary at the Department of Homeland Security and now in private law practice.

"If anybody is going to release irresponsible, unlimited attacks, you'd expect it to be Iran."

National security experts have long complained that the administration should be more open about what the military could and would do if the United States were to be the victim of cyberattacks. They argue that such deterrence worked in the Cold War with Russia and would help convince would-be attackers that an assault on America would have dire consequences.

Mr. Panetta took the first steps toward answering those critics in a speech that analysts said was a thinly veiled warning to Iran and the opening salvo in the campaign to convince Tehran that any cyberattack against America would trigger a swift and deadly response.

"Potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests," he said in a speech in New York to the Business Executives for National Security.

While he did not directly connect Iran to the Gulf cyberattacks, he warned that Iran's abilities were expanding.

The presumed Iranian cyberattacks hit the Saudi Arabian state oil company Aramco and Qatari natural gas producer RasGas using a virus, known as Shamoon, which can spread through computers networks and ultimately destroy files by overwriting them.

In his speech, Mr. Panetta said the Shamoon virus replaced crucial system files at Aramco with the image of a burning U.S. flag. He said it also overwrote all data, rendering more than 30,000 computers useless and forcing their replacement. He said the Qatar attack was similar.

"This one worries me," said Richard Bejtlich, chief security officer for the Virginia-based cybersecurity firm Mandiant.

"I'm not an alarmist, but when I saw that 30,000 computers at Saudi Aramco got just deleted, that was a big deal. You don't see the Chinese government, you don't see the Russian government, or even their patriotic hackers go out and delete anything, for the most part."

From the Iranians' point of view, however, attacks against the United States may be justified because they have been hit hard by American sanctions leveled on their country because of its suspected nuclear weapons program.

Iran also believes that the United States and Israel were behind the Stuxnet cyberattack that forced the temporary shutdown of thousands of centrifuges at a nuclear facility there in 2010.

Frank Cilluffo, , a former special assistant for homeland security to

President George W. Bush, said U.S. authorities have suspected Iran of trying to plot cyberattacks against American targets, including nuclear plants. He said that Iran's Revolutionary Guard Corps appears to now be trying to bring some hacker groups under its control.

"Iran has been doing a lot of cyber-saber-rattling," said Mr. Cilluffo, now director of George Washington University's Homeland Security Policy Institute. "What they lack in capabilities, they more than make up for in intent."

Cyber criminals target small businesses

Source: http://www.informationweek.com/byte/personal-tech/science-technology/how-small-business-owners-become-cyber-v/240009082

Many people do not think of cyber criminals or hackers when they are on the Internet doing business or just browsing for fun. People who run small businesses think largely the same way.

A recent study conducted by the National Cyber Security Alliance and Symantec found that 77 percent of small business owners in the United States think their company is safe from cyber criminals. Trouble is, 83 percent of them do not have a cyber security plan.

BYTE reports that the main issue is that small businesses do not know what to do with critical information they have stored on their computer and mobile systems. Cyber threats on businesses can come from several places — the most popular being outside the organization from a hacker, or from within the organization when an employee or ex-employee steals data.

Ellen Richey, chief enterprise risk officer Visa Inc, said small businesses that conduct their transactions online with debit and credit cards, leave themselves exposed in more than one way. They could be at risk from thieves who are attempting to steal their information, or from a hacker who steals someone else's identity or credit card and makes purchases with it.

Consumers can also be at risk, especially if they are using social networks to post information about themselves.

Hackers are using social engineering more often as a way to get into a customer's account, according to Richey.

"We at Visa want to make security important to small businesses by getting data out of their system," Richey told *BYTE*. "by moving to a dynamic data system. That way, even if a cyber criminal stole a card number, the person still couldn't use it to commit fraud.

"If we had that fully in place that would reduce the opportunity to commit fraud because small businesses wouldn't have valuable data anymore. In the future, only the big aggregators of data — like Visa itself, will have vulnerable data."

Richie offers five tips for establishing a cyber security policy (see also Visa's Security Sense page)::

- Not knowing what data you even have and where it is can put you at risk. Know the who, what, where, of your sensitive data and what kind of payment data you actually have, where it is, and who has access to it. This enables you to know where your risk is.
- If you do not need the data, don't keep it. Companies tend to store payment information on their laptop. They may even allow employees to access it on their own devices, which become more likely with the BYOD trend. However, there are cloud services available for payments and encryption. For instance, Visa is coming out with a way to store secure data, including a point-to-point service and tokenization service.
- Outsourcing a secure solution provider can often introduce vulnerabilities. For instance, if a company hires a sales person from an outside company and that person comes in and installs the payment application on the computer system — and forgets to change the password. The most common mistake is leaving in place the default password. The problem usually occurs because the companies have outsourced the project to a reseller. It is not clear who is responsible for changing the password.
- Use secure devices and applications when accepting payments — Visa maintains a list of those gadgets on its web site. Small business owners can go and look and see what meets the standard. There are compromised applications that they should avoid still in the market place, so it's better to be aware of the risks instead of being ignorant to them.
- For payments specifically, there are certain tools that small business owners could use for verification, which include the code on the back of the credit card, address verification, or even install a physical space upgrade to EMV chip technology that will allow consumers to pay with smart cards.

In addition to education and awareness, technology can help close the gap in security and payment systems. For example, Mastercard and Intel recently announced that it is implementing PayPass, a near field communication technology in their Ultrabooks, allowing users to make online payments by tapping a card or their phone on their Ultrabook. Facebook, which has been conducting transactions online for years, has a system that allows you to use two separate forms of identification.

The methods for small businesses to protect themselves are out there, but small business owners must become aware of them or face the threat of having their systems hacked and losing important information, losing their customers information, or having their information put on the internet.

Kaspersky Lab working on a secure operating system for critical infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20121023-kaspersky-lab-working-on-a-secure-operating-system-for-critical-infrastructure

Antivirus firm Kaspersky Lab is set to make a major contribution to the security of critical infrastructure systems by developing an operating system specifically designed for such systems.

Eugene Kaspersky wants his OS to protect information used in infrastructure such as nuclear power plants, transportation control facilities, gas and electrical systems, and other "critically important" facilities. *PCMag* reports that the firm is currently in talks with industrial control system operators and vendors.

The KL OS is "highly tailored, developed for solving a specific narrow task," Kaspersky said in a

blog post, adding that the OS is not intended "for playing Half-Life on, editing your vacation videos, or blathering on social media."
Kaspersky says he wants his system to keep hackers and invaders from "any behind-the-scenes, undeclared activity."
"This is the important bit: the impossibility of executing third-party code, or of breaking into the system or running unauthorized applications on our OS; and this is both provable and testable," Kaspersky wrote.
The security of infrastructure has become paramount in many countries as the threat of attacks – and, in some cases, actual attacks — by terrorists, spies, and the militaries of rival nation-states has increased substantially in recent years. There are growing worries about the ability of foreign countries being able to shut down or severely disrupt systems on which the economies and well-being of industrial countries depend. In his blog post, Kaspersky mentioned a situation in Queensland, Australia in which a hacker flooded an area with sewage in revenge for a local firm declined to hire him for a position. It took officials months to realize they were hacked.
"This is the important bit: the impossibility of executing third-party code, or of breaking into the system or running unauthorized applications on our OS; and this is both provable and testable," Kaspersky wrote in his blog.
Kaspersky did not give out many details on the project as he does not want competitors to "jump on our ideas and nick the know-how." There is no word on when the OS will be completed or when the lab will release it, but Kaspersky said more details will be released in the near future.

CHAMP missile test flight knocks out electronic devices with a burst of energy

Source:http://www.gizmag.com/boeing-champ-missile-test/24658/?utm_source=Gizmag+Subscribers&utm_campaign=00e0512733-UA-2235360-4&utm_medium=email

This week (end of Oct, 2012), science fiction became science fact as a Boeing CHAMP missile knocked out a building full of electronics in the Utah desert at Hill Air Force Base. There was no explosion and no flying shrapnel. There was only the sound of the missile's engine as it flew overhead and the sputtering of sophisticated computers crashing as they were hit by a beam of high-energy microwaves.

CHAMP, which stand for Counter-electronics High-powered Microwave Advanced Missile Project, is a cruise missile that replaces an explosive weapon with a sort of "death ray" for electronics. The effect is similar to Electromagnetic Pulse (EMP) bombs that show up in James Bond films and give military planners nightmares about computer networks being disabled in a split second.
The difference is that where an EMP weapon uses a nuclear warhead or an explosive shot through a wire coil to generate a pulse over an area, the Boeing CHAMP missile aims a precise beam of high-energy microwaves at a target, or multiple targets, as it flies over.

The military advantages of such a weapon are obvious. "This technology marks a new era in modern-day warfare," said Keith Coleman, CHAMP program manager for Boeing Phantom Works. "In the near future, this technology may be used to render an enemy's electronic and data systems useless even before the first troops or aircraft arrive."

Monday's test, carried out in conjunction with the U.S. Air Force Research Laboratory (AFRL) Directed Energy Directorate, Kirtland Air Force Base, New Mexico, used a two-story building filled with electronics as the primary target. As the missile flew over in a pre-programmed course, it blasted the building with microwaves.

In seconds, the computers and other electronics inside were knocked out and even the cameras to record the test were rendered inoperative. That day, seven targets were hit and their electronics were disabled by the microwave beam before the missile flew to an "undisclosed location" and returned to Earth.