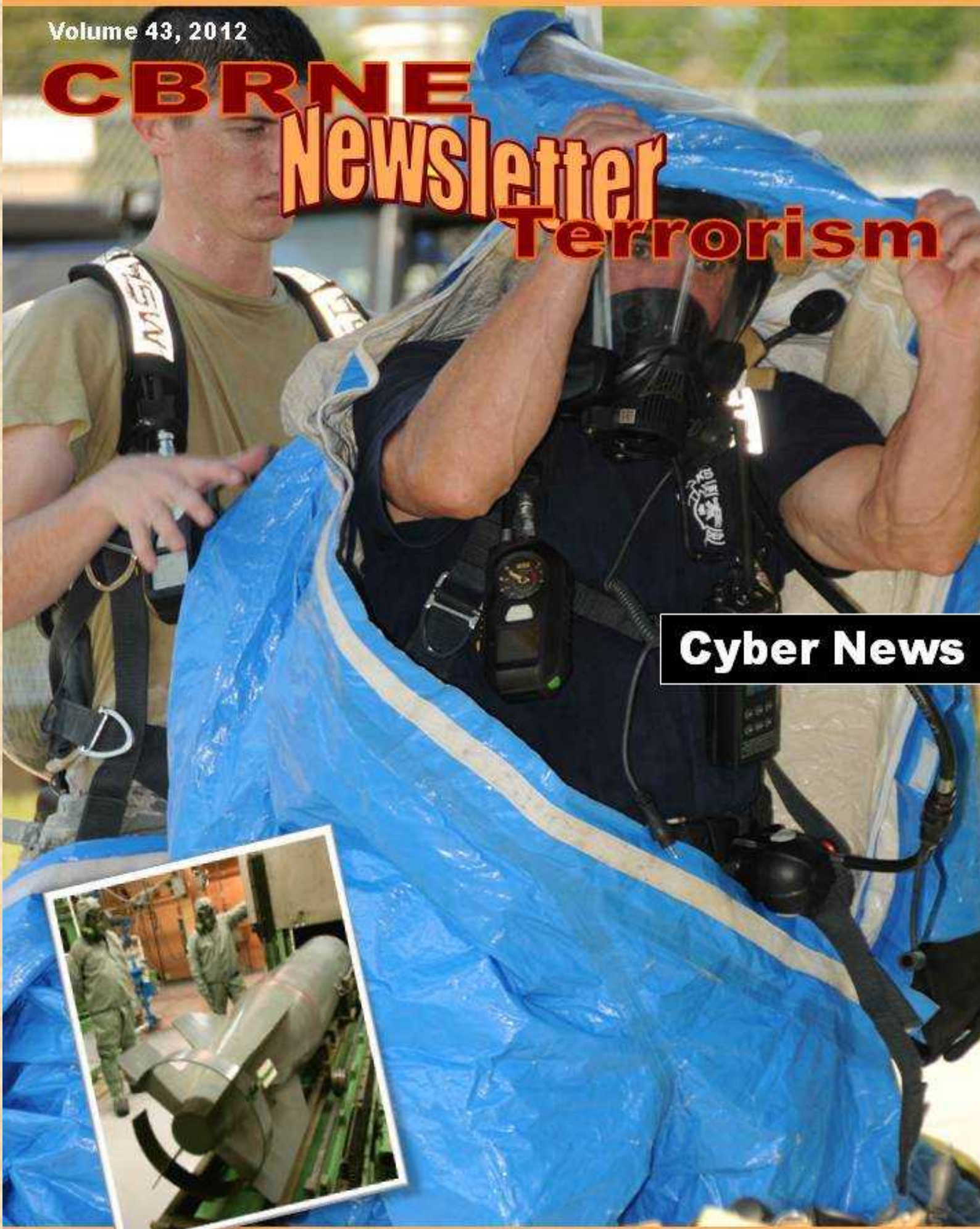
Syria's WMDs – Are they under control?

Volume 43, 2012

CBRNE Newsletter Terrorism



Cyber News

www.cbrne-terrorism-newsletter.com

How much does cybercrime cost?

Source: http://www.cam.ac.uk/research/news/how-much-does-cybercrime-cost/

The cost of protecting ourselves against cybercrime can far exceed the cost of the threat itself. This is the conclusion of a recent report 'Measuring the cost of cybercrime' by an international team of scientists led by the University of Cambridge.

On the basis of the findings – which provide the first systematic estimate of the direct costs, indirect costs and defence costs of different types of cybercrime for the UK and the world – the authors conclude that we should spend less in anticipation of cybercrime and more on catching the perpetrators.

"Advances in information technology are moving many social and economic interactions, such as fraud or forgery, from the physical worlds to cyberspace," said lead author Ross Anderson, Professor of Security Engineering at the University of Cambridge's Computer Laboratory. "As countries scramble to invest in security to minimise cyber-risks, governments want to know how large that investment should be and where the money should be spent."

However, many of the existing sources of data have either under- or over-inflated estimates of the scale of this risk explain the researchers.

For instance, a report released in February 2011 by the BAE subsidiary Detica in partnership with the Cabinet Office's Office of Cybersecurity and Information Assurance suggested that the overall cost to the UK economy from cyber-crime is £27 billion annually, a figure that many industry experts have questioned as being too high and lacking in methodology.

In the new study, the initial impetus for which was a request by the UK Ministry of Defence, the team of researchers has specifically avoided giving a single figure for the cost of cybercrime because the total depends critically on what is counted. They suggest that fraud within the welfare and tax systems – increasingly performed in the 'cyber' world – cost each citizen a few hundred pounds a year on average. Fraud associated with payment cards and online banking costs just a few tens of pounds a year; however, the fear of fraud by businesses and consumers is leading some to avoid online transactions, imposing an indirect cost on the economy that is several times higher.

By contrast, true 'cybercrime' – the new scams that completely depend on the internet – are only costing citizens an average of a few tens of pence per year directly. However the indirect costs, such as the money spent on anti-virus software, can be a hundred times that.

The report finds that each year the UK spends US$1 billion on efforts to protect against or clean-up after a threat, including $170 million on antivirus. By contrast, just $15 million is spent on law enforcement.

Overall, the study concludes that cybercriminals – often only a small number of gangs – are pulling in a few tens of pounds from every citizen per year, but the indirect costs to those citizens, either in protective measures such as antivirus or in cleaning up infected PCs, is at least ten times as much.

The Cambridge scientists, working with the econometrics of cybercrime in Cambridge's

Table 1: Judgement on coverage of cost categories by known estimates

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defence cost
Cost of genuine cybercrime							
Online banking fraud							
phishing	$16m	$320m	2007	$\times^{?}$	$\times^{?}$		
– malware (consumer)	$4m	$70m	2010	$\times^{\downarrow}$	$\times^{\downarrow}$		
malware (businesses)	$6m	$300m		$\times^{\downarrow}$	$\times^{\downarrow}$		
– bank tech. countermeasures	$50m	$1 000m	2010				$\times^{?}$
Fake antivirus	$5m	$97m	2008–10	×	×		
Copyright-infringing software	$1m	$22m	2010	×	×		
Copyright-infringing music etc	$7m	$150m	2011	$\times^{\downarrow}$			
Patent-infringing pharma	$14m	$288m	2010	×			
Stranded traveller scam	$1m	$10m	2011	$\times^{\downarrow}$			
Fake escrow scam	$10m	$200m	2011	$\times^{\downarrow}$			
Advance-fee fraud	$50m	$1 700m	2011	$\times^{\downarrow}$			
...							
Cost of transitional cybercrime							
Online payment card fraud	$210m	$4200m	2010		(×)		
Offline payment card fraud							
– domestic	$106m	$2100m	2010		$\times^{\downarrow}$		
– international	$147m	$2940m	2010		$\times^{\downarrow}$		
– bank/merchant defence costs	$120m	$2 400m	2010				$\times^{\downarrow}$
Indirect costs of payment fraud							
loss of confidence (consumers)	$700m	$10 000m	2010			$\times^{?}$	
– loss of confidence (merchants)	$1 600m	$20 000m	2009			$\times^{?}$	
PABX fraud	$185m	$4 060m	2011	×	$\times^{\downarrow}$		
...							
Cost of cybercriminal infrastructure							
Expenditure on antivirus	$170m	$3 400m	2012				×
Cost to industry of patching	$50m	$1 000m	2010				$\times^{?}$
ISP clean-up expenditures	$2m	$40m	2010			$\times^{?}$	
Cost to users of clean up	$500m	$10 000m	2012			$\times^{?}$	
Defence costs of firms generally	$600m	$10 000m	2010				$\times^{?}$
Expenditure on law enforcement	$15m	$400m	2010				×
...							
Cost of traditional crimes becoming 'cyber'							
Welfare fraud	$1 900m	$20 000m	2011	×	(×)		
Tax fraud	$12 000m	$125 000m	2011	$\times^{?}$	(×)		
Tax filing fraud	-	$5 200m	2010	×	(×)		
...							

Estimating costs and scaling: Figures in boldface are estimates based on data or assumption for the reference area. Unless both figures in a row are bold, the non-boldface figure has been scaled using the UK's share of world GDP unless otherwise stated in the main text. Extrapolations from UK numbers to the global scale should be interpreted with utmost caution. A threshold to enter this table is defined at $10m for the global estimate. Legend: × : included, (×) : partly covered; with qualifiers $\times^{\uparrow}$ for likely over estimated, $\times^{\downarrow}$ for likely underestimated, and $\times^{?}$ for high uncertainty.

colleagues in Germany, the Netherlands, the USA and UK, considered all the main types of cybercrime – online payment and banking fraud, fake antivirus, patent-infringing pharmaceuticals, 'stranded traveller' scams, and botnets (whereby vast numbers of computers are taken over by a 'botnet-herder' who then rents them out to others to commit crimes).

For each crime, the researchers not only collected the best figures for direct and indirect costs, but also for the cost of defending against it, as co-author Dr Richard Clayton, expert in Computer Laboratory, explained: "Take credit card fraud. Direct loss is clearly the monetary loss suffered by the victim. However, the victim might then lose trust in online banking and make fewer electronic transactions, pushing up the indirect costs for the bank because it now needs to maintain cheque clearing facilities, and this cost is passed on to society. Meanwhile, defence costs are incurred through recuperation efforts and the increased security services purchased by the victim. The cost to society is the sum of all of these."

Acknowledging that the study provides a static view of what is a highly changeable category of crime, the researchers nevertheless believe that their data provides "a proper start on the problem", one which they will continue to update as increasingly accurate data comes available. Clayton added: "The study provides a first attempt to pull all available data together. Previous studies have made rough assumptions and not fully explained the methodology they used."

The straightforward conclusion to draw from their study, say the researchers, is that we should spend less on defence and more on policing, as Anderson explained: "Some police forces believe the problem is too large to tackle. In fact, a small number of gangs lie behind many incidents and locking them up would be far more effective than telling the public to fit an anti-phishing toolbar or purchase antivirus software. Cybercrooks impose disproportionate costs on society and we have to become more efficient at fighting cybercrime."

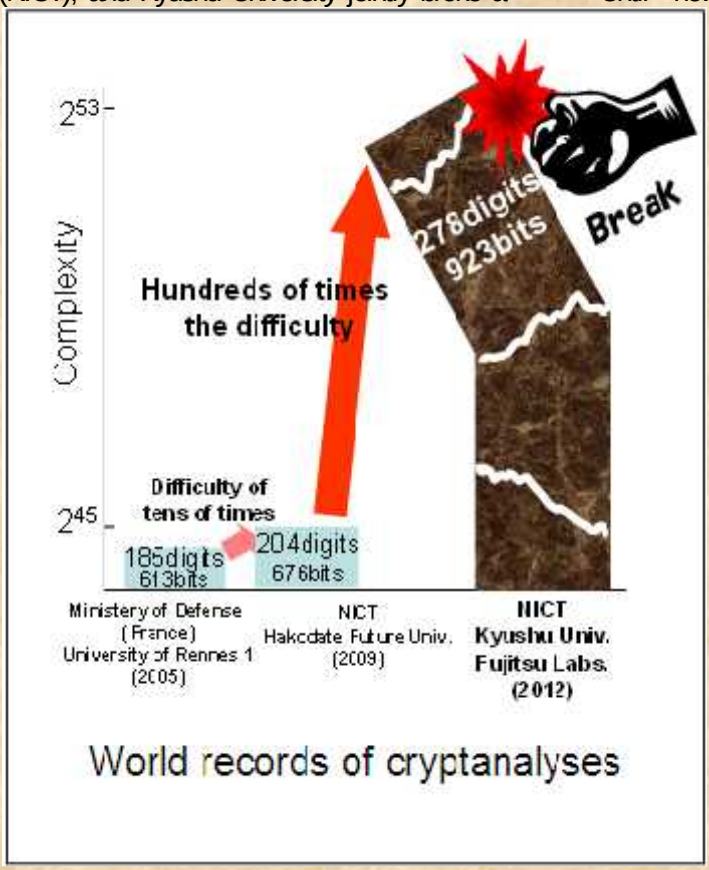
The report will be presented on June 25th at the Workshop on the Economics of Information Security in Berlin, Germany.

NOTE: You can download the full report from Newsletter's website – "CBRN-CT Papers" section

Researchers achieve world record cryptanalysis of next-generation cryptography

Source: http://www.homelandsecuritynewswire.com/dr20120619-researchers-achieve-world-record-cryptanalysis-of-nextgeneration-cryptography

Fujitsu Laboratories, the National Institute of Information and Communications Technology (NICT), and Kyushu University jointly broke a



world cryptography record with the successful cryptanalysis of a 278-digit (923-bit)-long pairing-based cryptography, which is becoming the next generation cryptography standard.

Until now, cryptanalysis of pairing-based cryptography of this length was thought impossible, as it was estimated to take several hundred thousand years to break. Despite numerous efforts to use and spread this cryptography at the development stage, it was not until this new way of approaching the problem was applied that it was proven that pairing-based cryptography of this length was fragile and could be broken in 148.2 days.

This result is used as the basis of selecting secure encryption technology, and is proving useful in the standardization of next-generation cryptography in electronic government systems in Japan and international standardization organizations.

Many cryptography systems are used from the viewpoint of information security on a modern information system. Recently, much attention has been paid to the new pairing-based cryptography system, which is being standardized as a next-generation

encryption system. The technology is attractive because it can be used for various useful applications such as identity-based encryption, keyword searchable encryption, and functional encryption, which were impossible using previous public key cryptography.

As cryptanalytic techniques and computers become more advanced, and cryptanalytic speed accelerates — cryptographic security decreases. Fujitsu says that it is, therefore, important to evaluate how long the cryptographic technology can be securely used. On the other hand, pairing-based cryptography has not advanced, so it was premature to evaluate its security against a new attack method.

As for a security evaluation of cryptographies, Fujitsu says its researchers succeeded with the cryptanalysis of the pairing-based cryptography of 278 digits (923 bits) by **using twenty-one personal computers (252 cores) in 148.2 days.** The cryptanalysis is the equivalent of spoofing the authority of the information system administrator.

As a result, for the first time researchers were able to proved that the cryptography of the parameter was vulnerable and could be broken in a realistic amount of time.

This was a challenging problem, as it required several hundred times computational power compared with the previous world record of 204 digits (676 bits). The researchers were able to overcome this problem by making good use of various new technologies, such as a technique optimizing parameter setting that uses computer algebra, a two dimensional search algorithm extended from the linear search, and by using their efficient programming techniques to calculate a solution of an equation from a huge number of data, as well as the parallel programming technology that maximizes computer power.

"This result is not just a new world record of cryptanalysis, "Fujitsu says. "It also means the acquisition of valuable data that forms a technical foundation on which to estimate selection of secure encryption technology or the appropriate timing to exchange a key length. We will continue to move forward on research that pushes the boundary of the secure use of cryptography."

Cyber-security and the Republic of Cyprus

New challenges and observations towards the development of a comprehensive cyber-strategy
By Nikolas Stylianou

Source: http://www.rieas.gr/research-areas/global-issues/balkan-studies/1788-cyber-security-and-the-republic-of-cyprus-new-challenges-and-observations-towards-the-development-of-a-comprehensive-cyber-strategy-.html

In the last years, cyberspace has been transformed into a distinct theatre of war operations, a sub-arena within the overall theatre of war which is characterized by its own norms, patterns and dynamics. Cyber-warfare is associated with the fifth dimension of defence with the rest four being the land, the sea, air and space. To the time, several states have developed cyber-security strategies and have incorporated cyberspace as an integral part of their national security strategies. Specifically, European states that have developed cyber-security strategies are Estonia, Finland, the Czech Republic, France, Slovakia, Germany, Lithuania, Luxemburg, the Netherlands and the United Kingdom. The United States, Canada, Japan, India, Australia and New Zealand set the puzzle in regards to the countries that have developed comprehensive cyber-security strategies.

The afore-mentioned list explicitly indicates the global recognition in regards to the emergence of challenges that affect the security of cyberspace. More countries are expected to extend the list of countries possessing cyber-security strategies in the coming years. Cyber-space is aptly called the battlefield of the 21st century.

The development of extremely sophisticated malwares-viruses like Stuxnet and Flame that believed to have caused severe damage to the nuclear ambitions of Iran has come to solidify the increasing importance of cyber-space in contemporary strategic planning.

According to a recent publication by the New York Times, the United States and Israel made use of their offensive cyber-warfare capabilities with an aim to slow down Iran's 'progress toward developing the ability to build nuclear weapons'. The current article aims to outline the new challenges to national/international security that have emerged from the demarcation of cyberspace as a distinct battlefield. Furthermore, this article will seek to underline the necessity for the Republic of Cyprus to develop a comprehensive cyber-security strategy in order to keep up with contemporary and future challenges to its national security.

Cyber-warfare and new challenges to (inter)national security

To begin with, we need to set out the scene in regards to the characteristics of cyber-warfare. Cyber-warfare is an asymmetrical threat due to:

- its inexplicit geographical orientation,
- its operational low cost
- it is bounded by no specific norms and patterns
- unpredictable and practically invisible

Cyber-warfare is a multi-dimensional threat and can potentially constitute a severe blow to the smooth functioning of a state. In the military level, cyber-sabotage may result to the interception of strategic/tactical intelligence, operational planning of the state, highly classified military information and data as well as the interception of telecommunications. In regards to the politico-military level, cyber-attacks may take the form of extended psychological and propaganda operations. In the economic level a cyber-attack can potentially paralyze any form of economic activity and generally affect the economic well-being of the state, ranging from the banking system to the state's sensitive economic data and reserves. In the social level, cyber-attacks may affect individual privacy and the interception of sensitive and private data.

Current estimations spin around the assumption that resources dedicated to the security of cyberspace will be multiplied in the next few years. This assumption lies on the fact that states become more dependent on cyber-space for their smooth-functioning. This may take the form of the digitalization of sensitive and confidential data ranging from issues of economic nature to issues of purely tactical military nature. The increased dependency of states on cyber-space will automatically create more vulnerabilities and gaps of security. However, the more states become vulnerable to cyber-security threats the more investments will be made in regards to the drafting, development and implementation of their cyber capabilities, defensive as well as offensive.

The cyber-era, the Turkish threat and the Republic of Cyprus

To the time, the Republic of Cyprus has not developed a comprehensive cyber-security strategy. It is a fact that the Republic of Cyprus is not as heavily dependent on cyber-space for the smooth-functioning of a state. However, the Republic of Cyprus will inevitably become more dependent in the next decade. The globe is experiencing the era of massive dissemination, distribution and publication of information. I strongly argue that due to the Turkish military threat, the Republic of Cyprus must proceed to the research and implementation of smart-defence methodologies that will enhance its defence capabilities against the multi-dimensional Turkish threat. The Republic of Cyprus exhibits limited deterrence capabilities due to the absence of substantial air-force and Navy. Hence, Cyprus relies heavily on its conventional military forces (National Guard) and the military support from Greece (air-fighters, submarines, battleships) which will operationally support National Guard in the case of a war incident with Turkey. However, the military sector of cyber-security and the Republic's military cyber-defensive capabilities is just an aspect of the overall cyber-security strategy.

Due to the multi-dimensional existential threat Turkey poses to the Republic of Cyprus, the latter must proceed to the establishment of a Centre for the Network Security of the Republic of Cyprus. In the last five years Turkey has made considerable advancements in regards to its offensive cyber-capabilities. The Turkish state has mobilized vast resources dedicated to cyber-security research and has developed infrastructure able to support its defensive and offensive cyber-capabilities. Due to the absence of a national centre for the countering of a massive cyber-attack, the Republic of Cyprus remains extremely vulnerable in the case of cyber-sabotage. Furthermore, due to the fact that cyber-attacks constitute a trans-

national threat, non-state actors are in a position to launch severe cyber-attacks against the Republic of Cyprus with an aim to undermine its economic or civil service network security. The aim of this contribution is to highlight the necessity for the establishment of a national centre for the countering of cyber-security threats against the Cypriot state. The proposed institution should be kept distinct from the purely cyber-security sector of the armed forces of the Republic of Cyprus. Hence, this centre will be responsible for the civil and private sector security and more specifically:

- the security of the government's communications network
- the civil service network security
- the banking sector's security in collaboration with banking institutions
- the security of the energy-power supply sector of the Republic
- the civil aviation network security
- the individual privacy/protection/security of cyber activity

For the purposes of the establishment of the afore-mentioned cyber-security centre, it is a prerequisite that the public and private sector collaborate smoothly. The private sector expertise and resources are fundamental for the success of such an emprise. In addition, the Republic of Cyprus must take the necessary steps to ensure collaboration with states which are in possession of advanced cyber-security defensive and offensive capabilities like Israel, France and Germany. It goes without saying that the establishment of such a centre will enhance and contribute to the overall security and smooth-functioning of the Republic of Cyprus, the private sector as well as in terms of individual cyber-privacy and security of transactions.

Nikolas Stylianou *is a RIEAS Research Associate, Security Analyst & PhD candidate in Security-Strategic Studies.*

Sharp increase in cyberattacks on U.S. critical infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20120703-sharp-increase-in-cyberattacks-on-u-s-critical-infrastructure

A new report from the U.S. Industrial Control System Cyber Emergency Response Team

(ICS-CERT) says that there has been a sharp increase in attacks on U.S. critical infrastructure between 2009 to 2011. The number of critical infrastructure incident reports ICS-CERT handled:

- 2009: 9 incident reports
- 2010: 41 incident reports
- 2011: 198 incident reports

Dark Matter reports that Of those 198, seven resulted in the deployment of onsite incident response teams from ICS-CERT, and twenty-one of the other incidents involved remote analysis efforts by the Advanced Analytics Lab.

The report notes that water sector-specific incidents, when added to the incidents which affected several sectors, accounted for more than half of the incidents. The report notes that that this is the result of the larger number of Internet-facing control system devices reported by independent researchers.

Kim Legelis, vice president of marketing at Industrial Defender, told *Dark Matter* that the magnitude of the increase was surprising. "While those of us close to critical infrastructure cyber security were aware of the escalating nature of the threat landscape, the level that this report validates was more severe than expected…. In addition, the report provides a baseline to compare future reports and incidents to in the future."

Despite the sharp increase in the number of attacks, the report notes: "No intrusions were identified directly into control system networks," the report states. "However, given the flat and interconnected nature of many of these organization's networks, threat actors, once they have gained a presence, have the potential to move

laterally into other portions of the network, including the control system, where they could compromise critical infrastructure operations."
The report says that in the seventeen onsite assessment ICS-CERT officials had to perform during the 2009-11 period – that is, in the seventeen most serious incidents – implementing best practices such as login limitation or properly configured firewall, would have deterred the attack, reduced the time it would have taken to detect an attack, and minimize its impact.
"Risk management and assessment is still an art, not a science," says Lamar Bailey, director of security research and development at nCircle, told *Dark Matter*. "We need a lot more collaboration between IT and security organizations to dramatically improve the accuracy of risk assessments."

Homeland security cites sharp rise in cyber attacks

Source: http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/

The companies that control critical infrastructure in the United States are reporting higher numbers of attacks on their systems over the past three years, according to a report issued by the Department of Homeland Security.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) says the number of reported attacks is up and attackers have been targeting companies with access to the country's power grid, water filtration facilities and a nuclear facility.
According to the report, which was released last week, there were 198 incidents reported to DHS in 2011, up from nine incidents in 2009. Cyber emergency response teams went to the physical locations to investigate and further analyze the threats in 17 of the 198 cases in 2011.
The most common threat was a technique known as spear-phishing, which can corrupt a company's computer system by uploading malicious attachments and gaining access to sensitive information. Eleven of the 17 incidents to which the emergency response teams physically responded were attacks that had been launched by "sophisticated actors," the report said.
The reported incident against a nuclear facility, which the department did not specifically name, was found to be the result of a USB drive that an employee had used to download presentation materials onto a laptop. Those materials included malware that was then able to spread to 100

hosts on the network, according to Homeland Security.

The government has made a point of not identifying companies by name due to fear that such public exposure would deter other companies who are the victims of similar attacks from coming forward and sharing information about the threats.

The report also identified common trends that allowed attackers to penetrate systems. They included employees who were not properly aware of potential dangers and technical and process flaws that left their systems exposed to attack.

The Department of Homeland Security sees the rise in the number of reported events as a sign that businesses are trusting the government more when it comes to allowing federal investigators to access their systems.

"Incident response is an essential part of cybersecurity," DHS spokesman Peter Boogaard said Wednesday. "DHS has made a consistent effort to work with public and private sector partners to develop trusted relationships and help asset owners and operators establish policies and controls that prevent incidents. The number of incidents reported to DHS's ICS-CERT has increased partly due to this increased communication."

The sensitivity over the public-private partnership remains a hotly debated issue in Washington, as lawmakers try to come up with legislation that would require acceptable minimum security standards for companies that operate critical infrastructure systems. Republican-backed proposals have included making the exchange of information between private companies and the government voluntary. Other initiatives, including a bipartisan bill backed by Sens. Joe Lieberman, I-Connecticut, and Susan Collins, R-Maine, would require companies to prove to the government that minimum security standards are in place, and would make that information subject to a government audit.

Cyber Reference Library

Source: http://www.nsci-va.org/CyberLibrary.htm

- NEW **ICS-CERT Incident Response Summary Report**; Industrial Control Systems Cyber Emergency Response Team; July 2012
- NEW **Cloud Computing Strategy**; Department of Defense; July 2012
- NEW **Report: World Cyber Security Technology Research Summit**; Centre for Secure Information Technologies; July 2012
- NEW **The Threat from Flamer**; European Network and Information Security Agency; June 2012
- NEW **Department of Defense Mobile Device Strategy**; Department of Defense; June 8, 2012
- NEW **Smart Grid Security**; European Network and Information Security Agency; July 1, 2012

- NEW Letter from top security guys to Senators Reid and McConnell; June 6, 2012
- NEW National Cyber Security Strategies; European Network and Information Security Agency; May 2012
- NEW McAfee Threats Report: First Quarter 2012; McAfee; May 2012
- NEW The Impact of Cybercrime on Business; Ponemon Institute; May 2012
- NEW 2011 Internet Crime Report; Internet Crime Complaint Center; May 2012
- NEW Electricity Subsector: Cybersecurity Capability Maturity Model; Department of Energy; May 31, 2012
- NEW Industry Affirms Commitment to Collaborative Effort to Combat Botnets; Industry Botnet Group; May 30, 2012
- NEW Attack Surface: Healthcare and Public Health Sector; National Cybersecurity and Communications Integration Center; May 4, 2012
- NEW 2012 Data Breach Investigations Report; Verizon; April 2012
- NEW Enabling Distributed Security in Cyberspace; Department of Homeland Security; March 23, 2012
- Cybersecurity and U.S.-China Relations; Brookings, February 2012
- NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow; Atlantic Council, February 2012
- NEW 2012 Threats Predictions; ; McAfee; January 2012
- Cyber-security: The vexed question of global rules; McAfee, January 2012
- Network Information Security in Education; European Network and Information Security Agency, January 2012
- National Strategy for Global Supply Chain Security; Executive Office of the President, January 2012
- NEW Network Information Security in Education; ; European Network and Information Security Agency; December 2011
- Trustworty Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program; Executive Office of the President, National Science and Technology Council, December 2011
- Cyber Security Aspects in the Maritime Sector; European Network and Information Security Agency, November 2011
- Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise; Department of Homeland Security, November 2011
- Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program; National Science and Technology Council, December 2011
- Joint Targeting in Cyberspace; Maj Steven J. Smart, USAF; Air and Space Power Journal, Winter 2011
- CYBERSECURITY HUMAN CAPITAL: Initiatives Need Better Planning and Coordination; GAO; November 2011
- The UK Cyber Security Strategy; Cabinet Office; November 25, 2011
- The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure; Project 2049 Institute: Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao; November 11, 2011
- Cyber Science and Technology Priority Steering Council Research Roadmap; Steven E. King; November 8, 2011

- Department of Defense Cyberspace Policy Report; Department of Defense; November 2011
- Foreign pies Stealing U.S. Economic Secrets in Cyberspace; United States Office of the Counterintelligence Executive, October 2011
- Internet Trends 2011; Mary Meeker; KPCB; October 18, 2011
- Recommendations of the House Republican Cybersecurity Task Force; October 2011
- Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements; GAO; October 2011
- Cyber Intelligence...setting the landscape for an emerging discipline; Intelligence and National Security Alliance; September 2011
- NEW Defending the networks: The NATO Policy on Cyber Defence; ; NATO; September 2011
- Cyber Events Since 2006; Center for Strategic and International Studies (CSIS); James Andrew Lewis; Updated September 9, 2011
- A Briefing on DOD's Cyber Organization and Challenges, GAO-11-75; GAO; August 30, 2011
- National Initiative for Cybersecurity Education Strategic Plan: Building a Digital Nation (DRAFT); NIST; August 11, 2011
- On Cyber Peace; Atlantic Council; Les Bloom and John Savage; August 8, 2011
- Cyber Security Strategy of the Czech Republic for the 2011 - 2015 Period; August 2011
- Mobilizing for International Action; EastWest Institute; August 3, 2011
- Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates; Government Accounting Office; July 29, 2011
- State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain; Government Accounting Office; July 2011
- Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities; GAO; July 25, 2011
- Department of Defense Strategy for Operating in Cyberspace ;Department of Defense; July 2011
- The Underground Economy of Fake Antivirus Software ; Stone-Gross, Ryan Abman Richard A. Kemmerer, Christopher Kruegel, Douglas G. Steigerwald, and Giovanni Vigna; University of California at Santa Barbara; July 2011
- Cybersecurity, Innovation, and the Internet Economy ;Department of Commerce Internet Policy Task Force; June 2011
- Cybersecurity Proposed Legislation; The White House; May 12, 2011
- International Strategy for Cyberspace; The White House; May, 2011
- Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities; United States Government Accountability Office; May, 2011
- 2011 State of Cyberethics, Cybersafety and Cybersecurity Curriculum in the U.S. Survey; National Cyber Security Alliance; May, 2011
- Retaliatory Deterrence in Cyberspace; Strategic Studies Quarterly; Eric Sterner; Spring 2011
- NEW Offensive Threat Modeling for Attackers: Turning Threat Modeling on its Head; ; Rafal Los and Shane MacDougall; May 2011
- Computer Network Incident Response and Reporting; Air Force Audit Agency; April 20, 2011

- DoD Cyber Operations Personnel Report ;Department of Defense; April, 2011
- Russia-U.S. Bi-lateral on Cybersecurity: Critical Terminology Foundations ; EastWest Institute; April, 2011
- National Strategy for Trusted Identities in Cyberspace; The White House; April, 2011
- Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action; Department of Homeland Security; March 23, 2011
- PRINCIPLES OF WAR FOR CYBERSPACE; Steven E. Cahanin, Lt Col, USAF; January 15, 2011
- Cybersecurity Two Years Later; Center for Strategic & International Studies; January, 2011
- Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure; Enterprise Strategy Group; November, 2010
- 2010 Report to Congress of the US-China Economic and Security Review Commission ; November, 2010
- Joint Terminology for Cyberspace Operations ; Joint Staff; November, 2010
- On Cyber Warfare ; A Chatham House Report: Paul Cornish, David Livingstone, Dave Clemente and Claire York; November, 2010
- Memorandum of Agreement Between the Department of Homeland Security and Department of Defense Regarding Cybersecurity ; Janet Napolitano and Robert Gates; October 13, 2010
- Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Recommendations, but Sustained Leadership Is Needed ; October 6, 2010
- Cyber Deterrence: Tougher in Theory than in Practice? ; Will Goodman; Strategic Studies Quarterly; Fall 2010
- Cyberwarfare and Its Damaging Effects on Citizens ; Stefano Mele; September, 2010
- Made in China: Waking Up to U.S. National Security Cyberthreats; The Asymmetric Net; September, 2010
- Vice Admiral Bernard J. McCullough, III, USN (Commander, U.S. Fleet Cyber Command, U.S. 10th Fleet); Testimony to The Terrorism, Unconventional Threats, and Capabilities Subcommittee on Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations; September 23, 2010
- Lieutenant General George J. Flynn, USMC (Deputy Commandant for Combat Development and Integration) ; Testimony to The Terrorism, Unconventional Threats, and Capabilities Subcommittee on Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations; September 23, 2010
- Major General Rhett Hernandez, USA (Assistant Deputy Chief of Staff) ; Testimony to The Terrorism, Unconventional Threats, and Capabilities Subcommittee on Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations; September 23, 2010
- Major General Richard Webber, USAF (Commander, 24th Air Force and Air Force Network Operations) ; Testimony to The Terrorism, Unconventional Threats, and Capabilities Subcommittee on Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations; September 23, 2010
- General Keith B. Alexander, USA (Commander, U.S. Cyber Command) ; Testimony to the House Armed Services Committee on U.S. Cyber Command: Organizing for Cyberspace Operations; September 23, 2010
- Cyberspace Operations: Air Force Doctrine Document 3-12; United States Air Force (July 15, 2010)

- United States Faces Challenges in Addressing Global Cybersecurity and Governance ; GAO (July 2010)
- A Human Capital Crisis in Cybersecurity ; CSIS (July 2010)
- Executive Cyberspace Authorities Act of 2010 (HR 5247 IH) (May 6, 2010)
- Advance Questions *(and answers)* for Lt Gen Alexander (Nominee for Commander, USCYBERCOM) (May 2010)
- Navy Vision for Information Dominance (May 2010)
- Net Generation: Preparing for Change in the Federal Information Technology Workforce; IT Workforce Committee (April 13, 2010)
- Cyber Vision and Cyber Force Development; Dr. Kamal Jabbour (March 2010)
- Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace; Testimony to Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security (November 17, 2009)
- The United States Air Force Blueprint for Cyberspace; Air Force Space Command (November 2, 2009)
- A Roadmap for Cybersecurity Research; Department of Homeland Security (November 2009)
- More Security, Less Waste: What Makes Sense For Our Federal Cyber Defense?; Testimony to Senate Committee on Homeland Security & Governmental Affairs: Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security (October 29, 2009)
- Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation; Prepared by Northrop Grumman Corporation for US-China Economic and Security Review Commission (October 9, 2009)
- Integrating Disciplines: Cyber Security, Law, & Policy; Georgetown University (October 1, 2009)
- Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress; Congressional Research Service: Catherine A. Theohary, John Rollins (September 30, 2009)
- Cyber Attacks: Protecting Industry Against Growing Threats; Testimony to Senate Committee on Homeland Security & Governmental Affairs (September 14, 2009)
- Air Force Cyberspace Mission Alignment; Secretary of the Air Force (August 20, 2009)
- Information Warfare: Assuring Digital Intelligence Collection; William G. Perry (July, 2009)
- Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations; Secretary of Defense (June 23, 2009)
- Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure; Melissa Hathaway (May 2009)
- Cyber Security: Developing a National Strategy; Testimony to Senate Committee on Homeland Security & Governmental Affairs (April 28, 2009)
- 2009 Data Breach Investigations Report; Verizon Business RISK Team (April 21, 2009)
- Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment; Intelligence and National Security Alliance (April 2009)
- Cybersecurity - Assessing Our Vulnerabilities and Developing an Effective Response; Testimony to Senate Committee on Homeland Security & Governmental Affairs (March 19, 2009)
- Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations; Congressional Research Service: John Rollins, Anna C. Henning (March 10, 2009)

- Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities; National Academies Press: National Research Council of the National Academies; William A. Owens, Kenneth W. Dam, and Herbert S. Lin (2009)
- Securing Cyberspace for the 44th Presidency; CSIS Commission on Cybersecurity for the 44th Presidency (December 2008)
- HPSCI White Paper on Cyber Security (December 2008)
- China's Electronic Long Range Reconnaissance; Timothy L. Thomas (Military Review Nov-Dec 2008)
- Cyber Attacks Against Georgia: Legal Lessons Identified; Cooperative Cyber Defence Center of Excellence (November 2008)
- Remarks by the Director of National Intelligence; Mr. Mike McConnel (Nov 2008)
- Emerging Cyber Threats Report 2009: Data, Mobility and Questions of Responsibility Will Drive Cyber Threats in 2009 and Beyond; Georgia Tech Information Security Center (October 2008)
- Cyber Threat to Critical Infrastructure 2010 - 2015; Peter D. Gasper (September 2008)
- Does EW + CNO = Cyber; Lt Col Jesse Bourque (September 2008)
- Cyber Storm II National Cyber Security Exercise Final Report; Australian Government; August 2008
- Defense Imperatives for the New Administration; Defense Science Board (August 2008)
- Cyberspace and the Changing Nature of Warfare; Kenneth Geers, U.S. Representative Cooperative Cyber Defence Centre of Excellence; Tallinn, Estonia
- CYBER ANALYSIS AND WARNING; GAO (July 2008)
- CHINA'S PROLIFERATION PRACTICES, AND THE DEVELOPMENT OF ITS CYBER AND SPACE WARFARE CAPABILITIES; HEARING BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION ONE HUNDRED TENTH CONGRESS SECOND SESSION (May 20, 2008)
- Statement of Franklin D. Kramer before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats (April 1, 2008)
- CYBERSPACE DOMAIN: A WARFIGHTING SUBSTANTIATED OPERATIONAL ENVIRONMENT IMPERATIVE; COLONEL OLEN L. KELLEY (March 15, 2008)
- Determining Communication Shortfalls for Homeland Defense; MAJ Kevin P. Wilson; Strategic Insights (December 2007)
- Information Warfare: An Emerging and Preferred Tool of the People's Republic of China ; Dr. William G. Perry; The Center for Security Policy; October 2010
- CRS Spyware: Background and Policy Issues for Congress; Updated September 26, 2007
- Flying and Fighting in Cyberspace; Sebastian M. Convertino II, Lou Anne DeMattei, Tammy M. Knierim (July 2007)
- CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats; GAO (June 2007)
- Lessons Learned from the Russian-Estonian Cyber-Conflict; Packet Clearing House; June 2007
- Terrorist Capabilities for Cyberattack: Overview and Policy Issues; Congressional Research (January 22, 2007)
- National Strategy for Information Sharing (2007)
- Warfighting in Cyberspace; LTG Keith B. Alexander (2007)
- Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems; U.S. Department of Energy; September 2006

-
- National Military Strategy for Cyberspace; Department of Defense (December 2006)
- Federal Plan for Cyber Security and Information Assurance Research and Development; Interagency Working Group on Cyber Security and Information Assurance (April 2006)
- Power to the Edge: Command...Control...in the Information Age; DOD Command and Control Research Program (April 2005)
- Creating a National Framework for Cybersecurity: An Analysis of Issues and Options; Congressional Research Service (February 22, 2005)
- Developing Situation Awareness Metrics in a Synthetic Battlespace Environment (2005)
- Critical Infrastructure and Key Assets: Definition and Identification; Congressional Research Service (October 1, 2004)
- Virtual Threat, Real Terror: Cyberterrorism in the 21st Century; Testimony to Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security (February 24, 2004)
- Critical Infrastructure: Control Systems and the Terrorist Threat; Congressional Research Service (July 14, 2003)
- The National Strategy to Secure CYBERSPACE; The White House (February 2003)
- Building a Deterrence Against Strategic Information Warfare; Geoffrey S. French (June 2002)
- National Communications System: Ensuring Essential Communications for the Homeland; Office of the Manager, National Communications System (FY 2002)
- Five Dimensional (Cyber) Warfighting: Can the Army After Next be Defeated Through Complex Concepts and Technologies?; Robert J. Bunker (July 10, 1998)
- Toward Deterrence in the Cyber Dimension; President's Commission on Critical Infrastructure Protection (1997)

Latest open-source cybersecurity software approved for government use

Source: http://openssl.org/

The Department of Homeland Security Science and Technology Directorate (S&T) today announced the validation and availability of an open-source cybersecurity tool for securing information shared across the Internet. Government agencies required to use cryptographic software validated to Federal Information Processing Standards (FIPS), will now have access to Open Secure Socket Layer (OpenSSL v2.0), a free, publicly available security software that meets federal security guidelines.

"OpenSSL is a widely-used component in many software security applications," said Luke Berndt, DHS Program Manager for the Homeland Open Security Technology (HOST) program. The mission of the HOST program is to identify viable and sustainable open source solutions that support national cybersecurity objectives. "With this program available for government use, the nation's critical online information will be safer while the government will find greater cost savings."

The National Institute of Standards and Technology validated the Open SSL using the FIPS 140-2 security standard for testing cryptographic modules. This validation is required for **cryptography used to protect** sensitive or valuable data within the federal government. The validation process was funded by DHS S&T and other government agency and private sector

partners. DHS S&T's investment in the validation process for OpenSSL will help government users access the latest security software, and allow software developers to integrate OpenSSL into the products they offer to government clients," said Berndt. "This collaborative effort is a great example of how government and industry can both benefit from the use of open source software."

SILEX and proliferation

By R. Scott Kemp

Source: http://thebulletin.org/web-edition/features/silex-and-proliferation

In July, the US Nuclear Regulatory Commission (NRC) held its final hearing to license the world's first facility to enrich uranium on a commercial scale using lasers. For years, experts have warned that laser enrichment, known as SILEX (separation of isotopes by laser excitation), would be particularly good at making highly enriched uranium -- the ingredient needed to make nuclear weapons -- and that a commercial venture could stimulate proliferation. That's why the Federation of American Scientists, the American Physical Society, the American Association for the Advancement of Sciences, a former US nuclear-weapons lab director, at least two congressmen, and dozens of others have called on the NRC to perform a proliferation assessment before licensing the proposed plant. In response, the NRC claims that nonproliferation assessments are outside the scope of their statutory responsibilities. Turning the cheek to such a grave matter of national security is not sound governance. If Congress or the NRC fails to act in the next few weeks, the new license will be issued, ushering in a watershed moment for nuclear proliferation.

SILEX is being developed by Global Laser Enrichment (GLE), a shell company half owned by foreign corporations. Its novel technology is licensed from Australia's Silex Systems Ltd., which has been trying to commercialize its process for over 20 years. Silex Systems agreed in 1999 to subject itself to US government control through a treaty between the United States and Australia. That treaty allows the company to court American investors, but it also allows the US government to regulate whether the technology can be deployed. Indeed, the opportunity to take SILEX off the market was part of the nonproliferation reasoning behind the agreement. A decade later, the moment of truth has arrived.

Article Highlights

- SILEX is a new enrichment technology that happens to be well suited for making nuclear weapons. The benefits of commercializing SILEX are not yet established, but the proliferation risks are significant.
- Dozens of countries are poised to copy SILEX if a US project demonstrates that the technology can be built on a commercial scale. The technical barriers, to the extent they exist, are not likely to endure the test of time.
- The Nuclear Regulatory Commission has refused to consider the proliferation risk in its decision to issue a license for the first commercial SILEX facility, despite a statutory obligation to do so. Only a few weeks remain for Congress to intervene.

The proliferation problem

The concern with SILEX is that it is particularly suited for nuclear proliferation -- even better than centrifuges. A proliferation-scale centrifuge facility can be housed in a high school gym and run from a diesel generator. According to GLE, an equivalent SILEX plant would be 75 percent smaller and use less energy. SILEX can also enrich fuel-grade uranium to weapons-grade in fewer steps than a gas centrifuge, making Iran-style proliferation easier. Finally, SILEX produces no distinctive chemical or thermal emissions that would reveal a clandestine plant's location. A 1999 State Department nonproliferation assessment of SILEX stated that such a "facility might be easier to build without detection and could be a more efficient producer of high enriched uranium for a nuclear weapons program."

GLE admits to all these issues, but the company claims -- in a seven-page assessment it refuses to publish -- that its technology is no easier to build than the centrifuge alternative. However, nearly every major technical SILEX challenge stems from its particularly complicated laser, a technology that is among the most rapidly advancing areas in applied physics. A single breakthrough in,

say, high-power diode lasers would eliminate most of the challenge overnight.

Further, the hurdles GLE faces in developing a commercially viable technology are necessarily more difficult than those a rogue proliferator faces. A proliferation plant capable of making just one bomb per year could be a tiny fraction (0.0008) of the size of GLE's plant. Many technical challenges can be ignored if scale and efficiency aren't the main goals. That's why the Defense Intelligence Agency, in analyzing these programs, wrote: "These lasers … demonstrate the fact that low-budget academic research programs are capable of developing lasers suitable for limited-scale LIS [Laser Isotope Separation] of [Uranium-235], a fact that has ominous implications for the future proliferation of nuclear weapons."

SILEX could easily pose a proliferation threat comparable to or worse than centrifuges. However, even these arguments are a distraction from the more fundamental problem: Two viable paths to the bomb are worse than one.

If the US government is going to allow another proliferation pathway to emerge, that technology should at least provide public benefits over the alternatives; a responsible government would also require that those benefits outweigh the added proliferation risk.

Uncertain benefits

GLE claims its primary commercial interest in SILEX is its low operating costs. In 2006, Silex Systems set a goal for a cost of $30-$45 per SWU (kilogram separative work units) -- a target it now admits was pure conjecture. Compare this with the cost of centrifuge enrichment, which produces at between $10-$60 per SWU, depending on the labor costs and technology-set used. GLE's Rob Gereghty says the company has been working on a "test loop" since July 2009 but that studies on SILEX's commercial viability will take "years to complete." Nonetheless GLE wants a license to build a commercial-scale plant now -- without first demonstrating SILEX's viability or allowing the government to compare the undemonstrated commercial benefits against the inadequately studied proliferation risks.

Policy makers should also note that lower operating costs would not directly benefit the public, because the price of enrichment is not dependent on GLE's costs. Enrichment is not a competitive market, so even if SILEX can attain low operating costs, that figure only translates into greater profits for GLE and its foreign investors, not reduced prices for public utilities.

A commercial-scale SILEX facility doesn't seem to offer indirect benefits, either. Because of the contractual nature of the enrichment industry, SILEX is more likely to displace, rather than supplement, enrichment capacity at three already-licensed US enrichment plants -- leading to no net increase in US market share or the number of countries subject to US nonproliferation controls. Nor could SILEX be used to support domestic national security programs, because the treaty restricts it to civil applications. Clearly, an objective evaluation of benefits is needed before a plant is licensed.

US government response

While the NRC has often admirably ensured protections for public health and safety, it has so far refused to look at the critical question of proliferation. US law provides that the NRC "shall prescribe such regulations or orders as may be necessary or desirable to promote the Nation's common defense and security with regard to control, ownership, or possession of any equipment or device ... capable of separating the isotopes or uranium or enriching uranium." Proliferation would seem to be integral to "common defense and security." In March, lawyers at the Congressional Research Service issued an opinion affirming that the NRC does have the authority to require "an assessment detailing the proliferation risks." Nevertheless, the NRC says it "considers a nuclear nonproliferation impact assessment to be outside the scope of the agency's statutory responsibilities" as it pertains to "issues of international policy unrelated to the NRC's licensing criteria."

Instead, the NRC routinely cites the State Department's 1999 nonproliferation assessment, which analyzed proliferation risks before the United States entered the treaty. The implication being that the question at hand -- whether the NRC should license a commercial-scale facility -- has already been addressed. It has not. That assessment, completed years before GLE even existed, tackled the question of whether to leave SILEX to the Australians or form a treaty through which the US government would gain some control over SILEX. The State Department did not study whether the technology should be deployed

commercially or what the proliferation implications of such a deployment would be.
At best, the NRC is searching for creative ways to avoid a proliferation assessment. At worst, the NRC is violating US law by treating a nondiscretionary obligation as one that can be ignored.
Some American officials fear that, if the technology is not commercialized in the United States, Silex Systems will take its technology elsewhere. That's a valid concern -- but only to the extent that Australia is willing to aggravate the United States by terminating the treaty *and* that Silex Systems could find new ways to commercialize its technology using information not developed by GLE. Article 16(3) of the US-Australia treaty guarantees that any information developed or learned over the course of the GLE collaboration can never be used for a project located outside US territory, even after the treaty has been terminated.
Besides, concern that Silex Systems might go elsewhere is even more reason for the United States to take the risks seriously and give SILEX a fair trial. If it is established that SILEX really is a good idea, then commercialization can proceed. If, however, it turns out that SILEX is not cost competitive or that the proliferation risks outweigh the social benefits, then it will be established that no nation should develop SILEX and the United States and Australia can work together to mothball the technology and prevent proliferation -- something the State Department's own analysis implies Australia is likely to do, given "Australia's strong commitment to the NPT and other elements of the nuclear nonproliferation regime."

Ticking clock

According to the State Department assessment, "It seems likely that success with SILEX would renew interest in laser enrichment by nations with benign intent as well as by proliferants with an interest in finding an easier route to acquiring fissile material for nuclear weapons." At least 27 countries -- including North Korea and Iran -- have dabbled with laser enrichment. Recently, South Korea and China began courting US laser-enrichment experts, and in April India purchased a SILEX-type laser.
As GLE progresses, more sensitive information will leak, and more states will become interested in SILEX. It is time we study whether the benefits of this project outweigh the proliferation risks. There is plenty of time to conduct that study -- during GLE's "years" of pre-commercialization research. Meanwhile, the NRC can hold GLE's license, with final decision pending a positive nonproliferation review. When a nation's regulator fails to regulate, it leads to unforeseen and potentially catastrophic consequences. Unless Congress or the NRC commissioners intervene now, SILEX could become America's proliferation Fukushima.

Europe's quixotic plan to "clean" the Internet of terrorists

Source:http://arstechnica.com/tech-policy/2012/08/europes-quixotic-plan-to-clean-the-internet-of-terrorists/

Delegates from Germany, Spain, the United Kingdom, the Netherlands, Belgium, and Europol—the European Union's criminal intelligence agency—will gather in London this September as part of a project to cleanse the Internet (or at least the European section of the Internet) from "terrorist websites." And they have European Union money to do it.
The CleanIT project hopes to develop a flagging system for "terrorist" content. It wouldn't be mandatory, but Internet providers would be encouraged to take down or block the flagged material. The aim is to create "a non-legislative 'framework' that consists of general principles and best practices… to counter the illegal use of Internet," says the group.
But who is a terrorist? And what's a terrorist website? Would there be an appeal process? No one is really sure yet.
In May 2010, CleanIT received a €400,000 ($428,000) grant from the Prevention of and Fight against Crime Programme of the European Commission. When the project is scheduled to wrap up in February 2013, the result should be an "implementation guideline" of "principles."
"These principles can be used as a guideline or gentleman's agreement, and can be adopted by many

partners," the group states on its website. "They will describe responsibilities and concrete steps public and private partners can take to counter the illegal use of Internet."
This CleanIT campaign is spearheaded by But Klaasen, the Dutch national coordinator for counterterrorism and security.

"We feel that there is a gap between legislation and how the Internet works," he told Ars. "For a hosting company—it's hard for a company to evaluate something that's illegal. We cannot expect from the hosting company whether or not to evaluate whether it's illegal. At some point it's notified. What we try to do is to help them, to see in [these] cases what [the host] should do."
"There a lot of cases in Europe where terrorists are caught because of what they said on the Internet," Klaasen added. "In our country, having speech doesn't mean you have unlimited freedom. There are boundaries within freedom of speech. There are limits."

The limits of speech

European civil libertarians and digital activists have two main problems with CleanIT. First is their opposition on freedom of speech grounds. In the United States, citizens have the more-or-less blanket right to express ideas, and that includes hate speech. (Some limits do exist, especially with regard to encouraging violence.) The operating principle has generally been that undesirable speech should be countered with more speech, not less.
That's not the approach taken in Europe, where hate speech is most definitely not protected. Many European Union states (and even some non-EU countries in Europe) have various types of anti-hate speech legal mechanisms, in part to head off terrorism and far-right violence. But the CleanIT project would brand entire websites as illegitimate and call for their takedown. Is it the right precedent to set?
"If the European Union decides that extremist views do not belong on the Internet, will [it] then be all right for China, Indonesia and Syria to come to a similar decision?" wrote Willemien Groot in a December 2011 opinion piece on the website of Radio Netherlands Worldwide. "Every country will be able to ban what it decides are extremist views. Indonesia can quietly continue working on its own internal code of conduct that every Internet user will be forced to adhere to."
This, of course, is what already takes place. France was able to push Yahoo to remove the auction of historical Nazi material, various European courts have required website blocking of sites like The Pirate Bay, while Iran and China frequently top the list of countries that heavily censor and surveil their domestic networks. The real question isn't about whether this should happen—it already does—but where European nations should draw their own lines around online speech, and who gets to decide what's in and what's out.
"There is no fixed definition of what is extreme," said Arthur van der Wees, an IT lawyer in Amsterdam, in an interview with Ars. "If you look at the French Revolution, who was extreme? Was it the royalty or the other guys?"

Who needs a "law"?

The CleanIT project, should it actually move forward, might come into conflict with the Charter of the Fundamental Rights of the European Union. Under Article 11, the Charter states: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."
Further down, under Article 52, the Charter allows for various limitations to be legally imposed, but it reiterates that those restrictions must be "provided for by law and respect the essence of those rights and freedoms."
CleanIT doesn't want to create new laws, however.
Because of this, many digital rights organizations in Europe call the entire

project overbroad—and designed to circumvent existing judicial and legislative structures.

"There's no due process, no presumption of innocence," said Joe McNamee, the head of European Digital Rights, in an interview with Ars.

For the moment, CleanIT only has participants from the tech industry and government, and very little involvement from outside groups and from the public. That's one of the main problems that the Dutch online advocacy group Bits of Freedom has with the project.

"Any restriction on freedom of communications and privacy by the government must be based on formal law," wrote Rejo Zenger, one of the organization's leaders, in an e-mail sent to Ars. "This is a requirement set in the European human rights treaties. It's there for a reason: such rules must be created in full transparency and the parliament must be able to reject proposals when it sees fit."

The borderless Internet

More fundamentally, even if all the debates about speech and law can be worked out, practical concerns arise. What happens if a banned site simply moves its hosting outside the European Union—to Switzerland, Iceland, Serbia, Russia, Turkey, or even farther afield, to the United States or Japan?

Bits of Freedom is just one of the European organizations opposed to CleanIT

Klaasen admits that "there will be a problem indeed if the website pops up in a country where it is allowed. There we reach the limitations of this project. That's why it's limited to EU. We have the EU legislation as a base. The first step we can take is to have all the servers installed in Europe be cleared of illegal material."

"The name of the project is a bit too ambitious, but the subtitle—'reducing the impact'—is exactly what they're trying to do," said van der Wees, the Dutch lawyer.

Klaasen, like other CleanIT supporters, argues that such baby steps are better than nothing.

"Again, we don't have the ambition to solve the problem of terrorists' use of the Internet for the whole world," he said. "Even if we know that the Internet is a global thing and we're limited to European space—as a step, not a total solution—we know that in this case there's no way, legally, to fight it."

Simulation: what if digital WMDs attack America?

Source: http://www.kurzweilai.net/simulation-what-if-digital-wmds-attack-america

What would happen if terrorists or an enemy nation got their hands on digital weapons of mass disruption — like Stuxnet, Flame, or the newly reported Gauss — and used them to attack America?

How would it impact our economy, our banking system, our transportation system? How would IT organizations respond? Could we, in fact, defend ourselves?

"Those were questions I recently set out to answer," reports David Gewirtz for *ZDNet Government*. Over the course of three months, working with *The Economist*, he recruited an all-star team consisting of Roger Cressey, (former Director for Trans-national Threats on the National Security Council and Chief of Staff to the President's Critical Infrastructure Protection Board), Richard Clarke (former Special Advisor to the President on cybersecurity), Robert Rodriguez (former U.S. Secret Service Presidential protection supervisor and Homeland Security advisor), crisis PR expert Brenda

Christensen, and leading virus-threat expert Phil Owens.
They conducted a comprehensive simulation of such an attack, presented on June 6 at the Idea Economy: Information 2012 Summit in San Francisco.
The simulation began with three isolated events, three breakdowns in our transportation system. It then went deeper, looking at what would happen if an enemy could disrupt our overall transportation systems (specifically targeting older hardware and software), and how that could undermine trust and citizen confidence. The simulation then layered on additional threats. Next came a distributed denial of service attack against transportation Web sites and banks. Then came a coordinated cyberespionage attack, exploring what would happen if a worm could tunnel into our banking clearinghouse systems.
"There's nothing that would stop a major attack today… If there is a significant attack, we lack any ability to deal with it, not because we don't have the technology, but because we lack the political willpower, and because decisions have not been made to deal with it." — Richard Clarke, former Special Advisor to the President on cybersecurity.

Gauss Espionage Malware: 7 Key Facts

By Mathew J. Schwartz

Source: http://www.informationweek.com/security/attacks/gauss-espionage-malware-7-key-facts/240005296

What secrets does the newly discovered Gauss malware hide?

At a high level, Moscow-based Kaspersky Lab, which Thursday announced its discovery of Gauss, believes it "is a nation state sponsored banking Trojan," built using a code base that's related to Flame, and by extension Duqu and Stuxnet.
But the ongoing analysis of Gauss has yet to uncover the answers to numerous questions. For starters, as noted by Symantec, banking credentials are "not a typical target for cyber espionage malware of this complexity."
With that in mind, here are seven oddities and unanswered questions surrounding Gauss:

1. Malware Eavesdropped On Lebanon

Whoever heard of malware that came gunning for residents of Lebanon? Kaspersky said that by July 31, 2012, it had counted 2,500 unique PCs as being infected by Gauss since May, and traced 1,600 of those infections to PCs in Lebanon. The next most-infected countries were Israel (483 PCs infected), the Palestinian Territory (261), the United States (43), the United Arab Emirates (11), and Germany (5).

2. Espionage Malware Targeted Banks

According to Kaspersky's teardown of Gauss, the malware didn't just target Lebanon, but specific bank customers. "The Gauss code (winshell.ocx) contains direct commands to intercept data required to work with Lebanese banks--including the Bank of Beirut, Byblos Bank, and Fransabank," it said. But the malware also targeted users of Credit Libanais. Citibank, and eBay's PayPal online payment system.
In other words, Gauss may be the first known malware to have been commissioned by a nation state to spy on online banking customers. Then again, Jeffrey Carr, CEO of cyber risk management firm Taia Global, told Reuters that Lebanese banks have long been watched by U.S. intelligence agencies for their role in facilitating payments to drug cartels and extremist groups. "You've got this successful platform. Why not apply it to this investigation into Lebanese banks and whether or not they are involved in money laundering for Hezbollah?" he said.

3. Malware Module May Hide Stuxnet Warhead

Another curiosity: Kaspersky researcher Roel Schouwenberg said the "Godel" module found in Gauss may also include a Stuxnet-like "warhead" able to damage industrial control systems, reported Reuters.

4. But Gauss Avoided Stuxnet Mistakes

Gauss managed to avoid detection for over a year, by not infecting enough PCs to have been spotted by security firms. For comparison purposes, Gauss is known to have infected 2,500 PCs, compared with 700 for Flame, and just 20 for Duqu. Stuxnet, meanwhile, infected over

100,000 PCs, although security experts suspect that its creators--believed to be the United States, working with Israel--lost control of the malware due to a programming error, which let the malware spread outside of the single Iranian nuclear facility that it was meant to infect.

5. Banking Malware Prolific--For Targeted Attack

But the 1,600 Gauss infections--80 times the number seen for Duqu--place the malware in curious territory. "This is an uncharacteristically high number for targeted attacks similar to Duqu--it's possible that such a high number of incidents is due to the presence of a worm in one of the Gauss modules that we still don't know about," according to Kaspersky Lab. "However, the infections have been predominantly within the boundaries of a rather small geographical region," meaning that the malware is apparently only being used for targeted attacks, and carefully controlled.

6. USB Key Attack Code Copies Targeted Data

On a related note, Kaspersky said that Gauss is compatible with 32-bit Windows systems, although "there is a separate spy module that operates on USB drives ... and is designed to collect information from 64-bit systems." Interestingly, the malware installs a compressed, encrypted attack application onto USB drives, which only activates when it finds a targeted system.

"The spy module that works on USB drives uses an .LNK exploit ... [that is] similar to the one used in the Stuxnet worm, but it is more effective," according to Kaspersky Lab. "The module masks the Trojan's files on the USB drive without using a driver. It does not infect the system: information is extracted from it using a spy module (32- or 64-bit) and saved on the USB drive."

According to Symantec, the USB attack code would be quite difficult to spot. "Some sections of the payload binary that spreads to USB devices are RC4 encrypted with keys generated to target specific computers," it said, referencing the RC4 software stream cipher. "The underlying data has yet to be decrypted in these payloads."

7. Attack Code Installs Font

A substantial amount of Gauss analysis remains, before the design of its modules--or even how it goes about infecting systems--can be fully understood. In particular, "the infection vector is currently unknown," according to Symantec.

Another mystery is the Gauss module dubbed "Lagrange," which--as Symantec put it--"curiously installs a font called Palida Narrow." The custom TrueType font "appears to contain valid Western, Baltic, and Turkish symbols," according to Kaspersky. Why create custom fonts for malware? So far, that's just one more outstanding and unusual Gauss question that remains unanswered.

Rooting out rumors, epidemics and crime – with math

By Pedro C. Pinto, Patrick Thiran, Martin Vetterli

Source : http://www.pedropinto.org.s3.amazonaws.com/publications/locating_source_diffusion_networks.pdf

An EPFL team of scientists has developed an algorithm that can identify the source of an epidemic or of information circulating on a network. The method could also be used to help with criminal investigations.

Investigators are well aware of how difficult it is to trace things to their source. The job was arguably easier with old, mafia-style criminal organizations whose hierarchical structure more or less resembled a family tree.

In the Internet age, however, the networks used by organized crime have changed. Innumerable nodes and connections escalate the complexity of these network structures, making it ever more difficult to root out the source. Pedro Pinto, an EPFL postdoctoral researcher in the Audiovisual Communications Laboratory, and his colleagues have nonetheless developed an algorithm that could become a valuable ally for investigators, criminal or otherwise, as long as a network is involved. His research was published August 10, 2012 in the journal *Physical Review Letters*.

Finding the source of a Facebook rumor

"Using our method, we can find the source of all kinds of things circulating on a network, just be "listening" to a limited number of members," explains Pinto. Here's an example: suppose you come across a rumor about yourself, spread on Facebook and sent to 500 people – your friends, or friends of your friends. How do you find who started the rumor? "By looking at the messages received by just 15-20 of your friends, and taking into account the time factor, our algorithm can trace the path of that information back and find the source," he continues. This method can also be used to identify the origin of a spam message or a computer virus, using only a limited number of sensors.

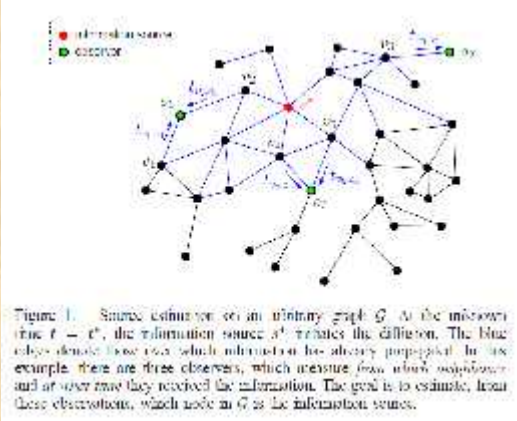


Figure 1: Source estimation on an arbitrary graph G. At the unknown time $t = t^0$, the information source s^0 initiates the diffusion. The blue edges denote those over which information has already propagated. In this example, there are three observers, which measure from which neighbour and at what time they received the information. The goal is to estimate, from these observations, which node in G is the information source.

Trace the propagation of an epidemic

Out in the real world, the algorithm can find the primary source of an infectious disease such as cholera. "We tested our method with data on an epidemic in South Africa provided by EPFL professor Andrea Rinaldo's Ecohydrology Laboratory," says Pinto. "By modeling water networks, river networks and human transport networks, we were able to find the spot where the first cases of infection appeared, by monitoring only a small fraction of the villages."

The method would also be useful in responding to terrorist attacks such as the 1995 sarin gas attack in the Tokyo subway, in which a poisonous gas spreads through the subterranean tunnels. "Using this algorithm, it wouldn't be necessary to equip every station with detectors; a sample would be sufficient to rapidly identify the origin of the attack and action could be taken before it spreads too far," claims Pinto.

Identifying the brains behind a terrorist attack

Computer simulations of the telephone conversations that would have occurred during the September 11, 2001 terrorist attacks were used as the basis of a test of Pinto's system. "By reconstructing the message exchange inside the 9/11 terrorist network extracted from publicly released news, our system spit out the names of three potential suspects – one of whom was found to be the mastermind of the attacks, according to the official enquiry."

The method thus has proven its validity *a posteriori*. According to Pinto, it could also be used as a preventive measure. "By carefully selecting points for making tests, we could more rapidly detect the spread of an epidemic," he thinks. It could also be a valuable tool for viral marketers, who use the Internet and social networks for advertising purposes. It would be easier for them to see –for example – which internet blogs are the most influential, and how their articles spread through the online community.

Contact:

Dr. Pedro Pinto, EPFL, Switzerland, Email: pedro.pinto@epfl.ch, Phone: +41 78 872 8200

Reference:

«Locating the source of diffusion in large-scale networks», by Pedro C. Pinto, Patrick Thiran, Martin Vetterli, *Physical Review Letters*, (**August 10, 2012)**