INFORMATION & SECURITY
An International Journal

Scenario-based Security Foresight

Edited by
Alexander Siedschlag

Procon Ltd.

Volume 29, 2013

Content *I&S*

The Way Ahead

I&S Monitor

Information & Security: An International Journal

Urciuoli, Männistö, Hintsa & Khan, vol.29, 2013, 51-68 http://dx.doi.org/10.11610/isij.2904

SUPPLY CHAIN CYBER SECURITY – POTENTIAL THREATS

Luca URCIUOLI, Toni MÄNNISTÖ, Juha HINTSA and Tamanna KHAN

Abstract: The same Information and Communication Technologies (ICT) that have contributed tremendously to the productivity of supply chain companies and governments alike, as well as to the global competitiveness of the European Union, expose modern societies to a range of cyber threats. ICT systems are fundamental to ensure that undisrupted flows of merchandise and critical supplies, such as oil, minerals, rare earths, pharmaceuticals and food are moved in and out of the EU territory. Past events have revealed the vulnerability of global supply chains to crime and terrorism. However, previous research does not highlight how these threats may be affected with the support of cyber attacks. Hence, by means of a literature review and experts' validation, this study develops a set of three scenarios that outline how cybercrime could jeopardize security of supply chains and, consequently, the well-being of European citizens. Finally, implications for managers and EU agencies are discussed.

Keywords: supply chain security, supply chain crime, cybercrime, cybersecurity, cyber threats.

Introduction

Cybercrime can be defined as any crime that is facilitated or committed using a computer, network, or hardware device; in particular, the computer or the device may be the agent, facilitator, or target of the crime that takes place in virtual or non-virtual places.[1] Security experts point out that cybercrime attacks are steadily increasing. Symantec has recently alerted that malicious attacks have increased by 81 % in 2011 compared to 2010.[2] 50 % of these attacks were targeting business sectors, in particular enterprises with less than 2 500 employees. This demonstrates that most probably criminals target smaller companies, the weakest links of the supply chains, where protection measures are not adequate. Still relevant data of larger companies, i.e. the supply chain focal companies, may be as well illicitly accessed and stolen.[2] Experts believe that in the future, attacks against business sectors will increase.[3] The motiva-

© ProCon Ltd., www.procon.bg. This article cannot be reprinted, published on-line or sold without written permission by ProCon.

tion may vary from monetary gains to hacktivism, i.e. sending a message "*to disrupt, embarrass, or make an example of their target—or all*".[4]

The consequences of cybercrime attacks are difficult to estimate, but it is evident that they may impact negatively both industries and our communities. Overall, these attacks result in loss of brand image.[4] It has been estimated that cybercrime is a more costly criminal phenomenon than the global trafficking in marijuana, cocaine and heroin (combined value $288 billion).[5] A survey in the UK performed in 1992 showed that the true level of losses from cybercrime was around £1.1 billion a year.[6] Another survey, conducted with Fortune 1000 companies in 1999, reported losses of more than 45 billion dollars related to theft of "*proprietary information.*"[7] A more recent survey, conducted in 24 countries worldwide, revealed that 431 million individuals were affected by cybercrime, causing an annual cost of $ 388 billion globally (including financial losses and time value loss).[8] In the US, costs of cyber attacks in 2011 were estimated to range between $5 000 and $188 000, with denial of service, web-based and malicious code attacks being the most expensive ones (Figure 1).[i,9]

As a consequence, during recent years, topics including cybercrime, cyber security, and cyber warfare have caught special attention and have been included in national security agendas of many countries around the world. On EU level diverse initiatives are being promoted to ensure the security of the critical infrastructure. For instance, the UK government allocated an extra of £500m to strengthen the protection of key in-

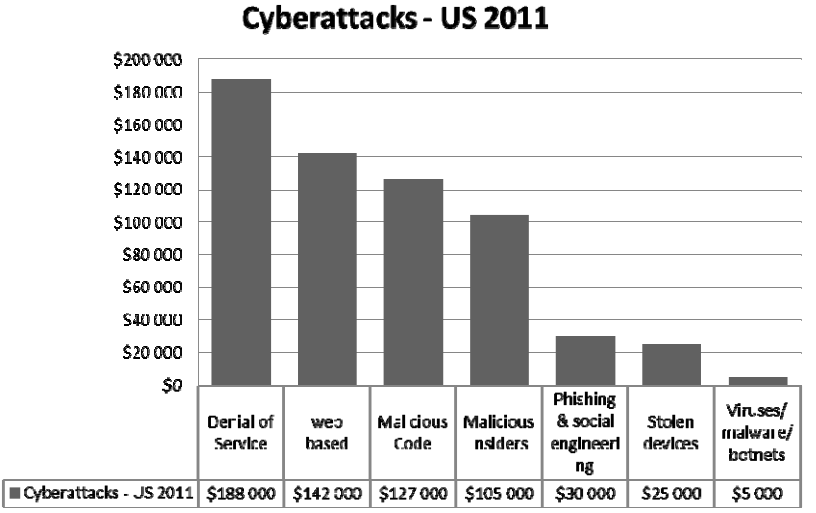

Figure 1: Costs of cyber attacks, US, 2011.[i]

[i] All figures include immediate losses and cost of investigation, interruption, and recovery.

frastructure and defence assets against cyber threats. In Sweden, the civil contingency agency has established a national operational coordination centre and is working actively to improve the capabilities to prevent, monitor and to recover from IT security incidents.[10] Likewise, in 2009 France created a national authority for cybersecurity (ANSSI, the French Network and Information Security Agency) and in 2011 issued a national strategy for the defence and security of information systems.[11]

The Importance of Cybercrime for Supply Chains

Cybercrime assumes a particular relevance if it is exploited to hit supply chains or their end-consumers, including citizens. Supply chains may be viewed as sets of virtual organizations that create a network or a pipeline in which services/products, information and finances flow through (Figure 2). In particular, it is well known that Information and Communication Technologies (ICTs) are very relevant to optimize supply chain management, operational routines (e.g. processes, production, distribution, etc.), as well as to guarantee the well-functioning of automated manufacturing systems.[12]

More specifically, IT systems and technologies find a wide variety of application in supply chain management, for instance:[13,12]

- Purchasing activities and order management
- Customer and supplier relationship management
- Demand and inventory monitoring and forecasting
- Manufacturing control and management
- Management of financial flows

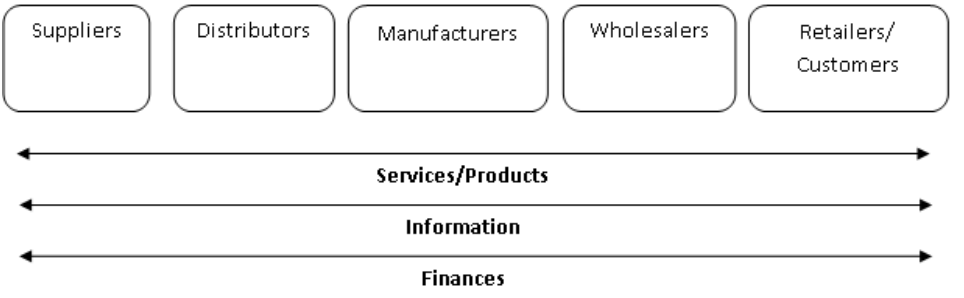

Figure 2: Integrated Supply Chain.[12]

- Monitoring and management of physical flows (e.g. fleet management systems, monitoring of environmental sensors), etc.

The main task of these systems is to establish electronic linkages and relationships with all the companies in the supply chain.[14] These systems may also improve the effective use of organisational resources, e.g. by replacing inefficient paper-based processes or by improving the performance of manufacturing systems.

Despite the beneficial effects, the information layer of supply chains can become a target for hackers or terrorists aiming to hit the European economy and community. For instance, by means of cybercrime, criminals may perform illicit activities as theft, sabotage, counterfeit, fraud, forgery, espionage etc.[15,16] An unauthorized intrusion in the information layer of oil supply chains could cause a black out of the ordering system and the consequent temporary stop of delivery of oil to Europe and energy production. Consequences could be even more serious if cybercrime is used as a means to manipulate or replicate the production of food or pharmaceutical supplies to and within Europe – an event that should not be seen as far away from reality in view of the latest discoveries of the Stuxnet, Duqu and Flame worms.[4,8,22] Hence, we wonder what are the real vulnerabilities of supply chains to cybercrime? How can these vulnerabilities be exploited to perform illicit activities (e.g. crime and terrorism)?

Very limited work has been found in relation to the topic analysed in this paper. Gabriole identified only some of the possible attacks on the electronic system and their importance for supply chains.[13] Bolhari develops a framework to describe pragmatically some of the main concepts of supply chain management information security.[7] Khan and Davis point out the importance for increased collaboration among IT and supply chain risk managers, in order to handle more efficiently cybersecurity threats.[17] However, none of the screened literature was depicting narrative scenarios describing how cyber threats may be used to perform illicit activities in supply chains.

Aim and outline

Hence, by means of a literature review, the purpose of this paper is to develop possible threat scenarios to enhance the understanding about how terror or criminal organizations may take advantage of IT vulnerabilities of supply chains not only for financial revenue purposes, but also to put at stake the safety of our societies. Thereafter, it is discussed how practical support may be given by governments to private operators to mitigate such risks.

The structure of the paper is the following: after the introduction, the method is described. Next, the results of the literature review and analysis are reported. Finally,

the results are discussed and the contribution to practitioners and scientific communities expounded.

Method

So far, the research on the topic addressed in this paper has been rather limited. Hence, our team decided to follow an exploratory approach – a qualitative research methodology aiming to discover and handle complex relationships and phenomena with the support of raw data and previous literature.[18] The literature framework was built by searching in existing databases the most prominent papers in the areas of information security, electronic supply chain management and EU bodies and legislations dealing with cyber threats. The searches in the literature were performed in search engines including Elsevier, Scholar and Emerald. Papers of interest were selected by screening the titles and abstracts and evaluating their relevance to this investigation.

Since very little has been found related to how cyber threats and techniques are used to commit supply chain crime we decided to review and report these two topics independently. Thereafter, the research team performed an internal workshop to combine them and try to develop scenarios describing how supply chain crime is committed with cybercrime. Among these scenarios, the team selected three scenarios that were expounded to three security experts for further review, criticism and feedbacks. The companies and organizations of the three security experts are the following:

- A global pharmaceutical company
- A national police organization
- A global company distributing supplies of clinical trials.

After a systematic round of review with the experts, the scenarios were improved by the team and finally reported and discussed in this study.

Literature Review

Cybercrime

Cybercrimes are classified in several ways. According to Gordon and Ford, cybercrimes can be classified in two types.[1] Type I cyber crime activities include, but are not necessarily limited to, phishing attempts, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud based upon stolen credentials. Type II cybercrime activities cover, among others, activities such as cyber stalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities online.[1]

Examining trends from 2009 to 2011, it may be noticed that the most frequent cyber threats may be associated to basic coding errors, e.g. buffer overflows, denial of service, arbitrary code execution,[ii] and format string vulnerabilities (Figure 3). However, it appears that these trends are of lesser importance in more recent years, 2010 and 2012.[4]

A particular category of cyber threats consists of attacks performed for espionage purposes. In 2011 these raised to 82 per day from the 77 per day of the previous year.[8] These kinds of attacks are worrying many industries and governments because they take advantage of the vulnerability of industrial control systems, supervisory control and data acquisition systems, i.e. ICS/SCADA systems.[4] Stuxnet, Duqu and Flame worms are recent examples of this specific trend.

The Stuxnet was discovered when it infected files controlling Siemens PLC (Programmable Logic Controller) devices, i.e. a digital computer used for automation of electromechanical processes to control machinery in factory assembly lines (e.g. valves, pipelines and industrial equipment). The virus may spread through infection of USB devices and directly attack the Siemens SCADA (Supervisory Control and Data Acquisition) control software installed on the infected Windows machines. In particular, the file infects the SCADA project files and also the Windows communication library to allow its installation on PLC devices once these were connected to

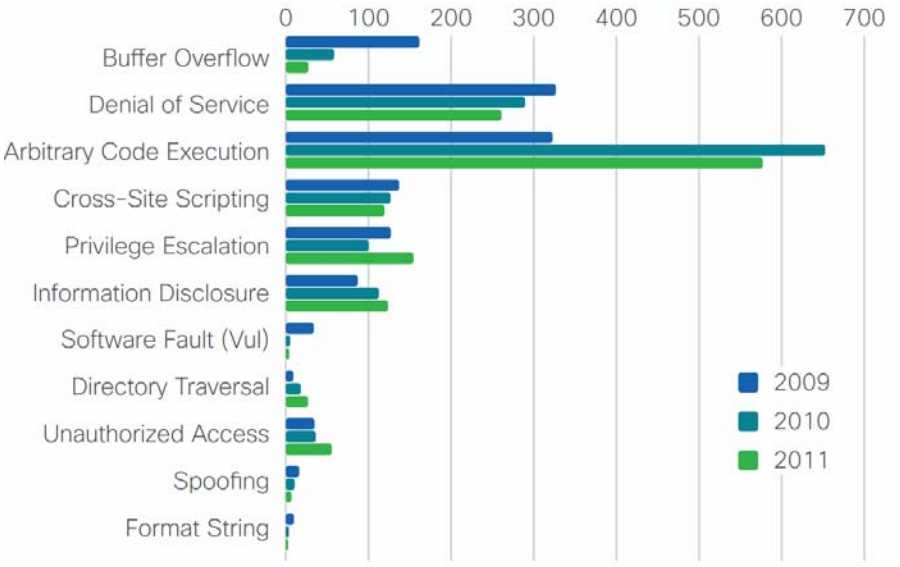

Figure 3: Vulnerability and Threat Categories.[4]

[ii] A software bug giving attackers the possibility to execute commands on host computers.

the infected computer via a data cable. The capabilities of such a virus are worrying, as production and manufacturing systems could be shut down or altered by closing valves and pipelines. For instance, production lines could stop or the final products could present modifications that could put the health of the final consumers into danger.[19] Initially the experts thought that the software was going to be used to blackmail industries or for espionage purposes. However, it was soon realized that it targeted only Siemens devices installed in only about 15 plants around the world. According to Symantec, of the machines found infected 60 % were in Iran, 18 % in Indonesia and 8 % in India.[8] Hence, a plot to sabotage the Iranian nuclear plan was suspected. The particular target was the Iran's uranium-enrichment plant in Natanz where apparently the infection disrupted the centrifuges' rotational frequency, shutting down uranium enrichment for a week.[20] Stuxnet attacked the same embargoed Siemens equipment that Iran managed to procure clandestinely.[21]

The Duqu is a computer worm whose purpose is to gather information from an infected machine. Experts believe that there is a strong relationship with the Stuxnet, since the Duqu is based on the same source code, and therefore suspicions that the same developers have produced the virus have been raised. Compared with Stuxnet, the Duqu searches and gathers information that could be useful to attack any kind of industrial and computer systems, not only Siemens PLC devices. Duqu seems also to be used to perform deleterious attacks, i.e. formatting hard drives, as well as to gather and steal information.[2]

Finally, Flame is a worm that has been recently discovered to have infected lots of computers, especially in the Middle East. Experts declare that Flame is probably even more sophisticated than Stuxnet appearing to be designed to specifically target Iran, leading to speculations on the involvement of the US and Israeli governments.[22]

Supply chain security

The topic of supply chain security has been widely studied in previous literature.[23] Different crime types take place in supply chains. These can be dependent on the cargo transport mode and type of cargo, the location of the attack as well as the degree of expertise of the criminal organizations.[24,25] Typical supply chain security threats can be classified in three different categories, these are: 1) economic crime, 2) ideological, political, ad-hoc, up/downstream and 3) facilitating crime.[26]

In Figure 4 we report data collected from an EU FP7 research project, showing the major crimes encountered by supply chain stakeholders in Europe during recent years. The following was indicated: theft in transit (23 %), data theft/cybercrime (11 %), bogus companies (10 %), and insider fraud (10 %). Additional relevant crimes that have been indicated during the data collection process include: smuggling

(9 %), counterfeiting (9 %), and terrorism (6 %).[iii] Other crime threats that were less frequently indicated by the respondents are illegal immigration (5 %), sabotage (5 %), product diversion (5 %) and product specification fraud. Finally, in very few occasions environmental crime was pointed out as a significant crime threat (2 %).[26]

EU Institutions, Regulations and On-going Research

Over the past years, the EU has taken substantial steps to formulate integrated policies designed to enhance protection of European Critical Infrastructure (ECI) and in this way reduce their vulnerability for a variety of threats including terrorism, criminal activities and natural disasters. In particular, the introduction of a legislative framework—the European Programme for Critical Infrastructure Protection (EPCIP)

Table 1: Cargo crime classified in 3 groups.[26]

1. Economic crime (revenue generating and/or cost saving)	*2. Other crime types: ideological, political, ad-hoc, up/downstream*
• Theft (including robbery, larceny, hijacking, looting, etc.) • Organized immigration crime (human trafficking, illegal immigration) • IPR violations and counterfeiting • Customs law violations (tax fraud, prohibited goods) • Other tax fraud (including sales tax / VAT) • Other fraud (including insurance, commercial contracts, etc.) • Other government agency law violations • Parallel trade • Environmental crime (pollution, wildlife) • Sea piracy • Extortion, blackmailing	• Terrorism (attacking supply chain, exploiting supply chain, etc.) • Sabotage • Vandalism • Gross negligence (with criminal charges) • Supplier crime(s), raw material fraud etc. • Sales channel crime(s), violations, fraud, etc.

3. Facilitating other crime(s)		
• Document forgery	• Identity theft	• Espionage
• Bogus companies	• Cyber crime	• Corruption

[iii] "Other" in Figure 4 includes war/riots, corruption, kidnapping and shoplifting, which were considered to be beyond the scope of the LOGSEC project.

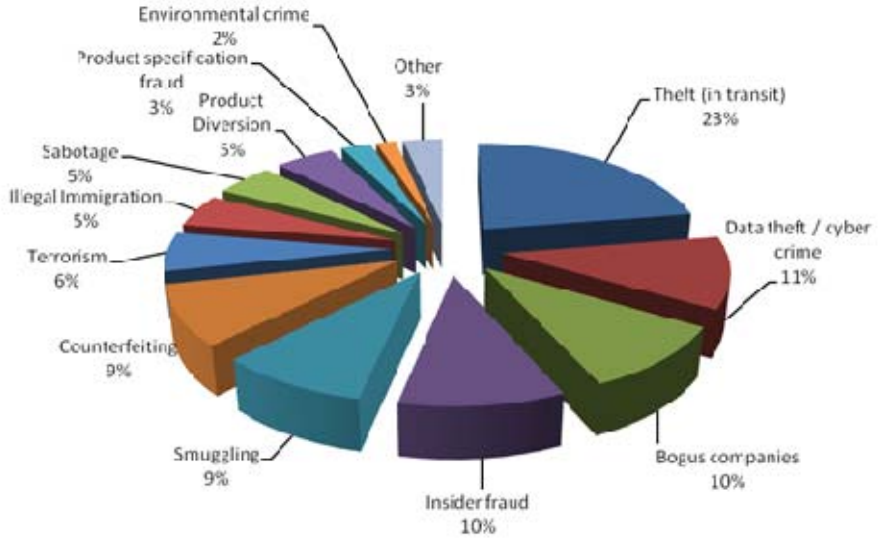

Figure 4: Present Crime threats[iv] (N=36 companies, referring to 12 crime types + Other)[26]

—designates common procedures to identify Critical Infrastructures in EU member states. In particular, the Council directive 2008/114/EC "*Identification and designation of European critical infrastructures and the assessment the need to improve their protection*"[27] obliges the member states to identify and designate European critical infrastructure in transport and energy sectors. Within the ICT sector a fundamental role is played by the European Network and Information Security Agency (ENISA) as it is in charge for the development of European-level cyber security programmes and Critical Information Infrastructure Protection policies.[27]

On European level the cyber security issue is also being exhaustively investigated in diverse FP7 research projects. It is possible to notice that these projects have a core focus on ensuring the security of the public infrastructure:

- *Forward*. An interesting result of the Forward project is the identification of eight categories of cyber threats: networking, hardware and virtualization, weak devices (RFID vulnerability), complexity, data manipulation, attack infrastructure, human factors, insufficient security requirements. Using these categories, diverse cyber threats scenarios are developed. From the perspective of supply chain security, industrial espionage is particularly interesting

[iv] Calculated as the proportion of a total of 120 references to the various threats mentioned by 36 respondents.

among them. The hypothetical scenario considers the infiltration of hackers in the IT layer of DALES. The scope of the attack is 1) to gain control of the development and production of remote-controlled aerial drones and 2) deploy a Trojan horse in the drones.[28]

- *Aniketos.* Aniketos develops a secure service development framework. This is accomplished by means of tools and methods that allow developers to identify cyber threats at design time by considering business, social and organizational mechanisms.[29]
- *SySSec.* SySSec is a Network of Excellence in the field of systems security for Europe. One of the main challenges that this research centre is undertaking is to proactively understand how to work with predicting threats and vulnerabilities and thereby build the defence accordingly. Specific objectives include the promotion of cyber security educational activities, establish think-tank to discover current and future cyber threats and create a roadmap in the area. In particular, the project highlights current and emerging threats in cyber attacks: social engineering, web-services and applications, bid data and privacy (data collection and aggregation), critical infrastructure, threats to smart mobiles and devices, insiders and network attacks.[30]
- *Tclouds.* The provision of cloud computing services has been steadily increasing during the last years. However, the progress made requires that developers cope with cyber attacks and show that these systems are not vulnerable. Hence, the project aims to improve the security, privacy and resilience of cloud infrastructure in a cost efficient manner and to demonstrate improvements in two key application areas: energy and healthcare.[31]

Results

As a first result our team performed an internal workshop to combine possible IT security threats with typical supply chain security threats. The result of this exercise is shown in Table 2. Supply chain security is a sub-domain in organizations' general supply chain risk management strategy.[32] Supply chain security management aims to specify, asses and mitigate risks of deliberate criminal activities intending to damage or destruct cargo, supply chain infrastructure or associated personnel; disrupt or disturb supply chain operations; steal cargo, hijack vehicles or capture associated personnel; or exploit supply chains for smuggling. Cybercrime is a key driver and facilitator of supply chain related criminal activities. The threat of cybercrime for the transportation and logistics industry will increase also in the future.[33] This trend will most likely cement the position of supply chain cyber security as a core component in the organizations' overall supply chain security strategy.

Cybercrime techniques, such as phishing and hacking, enable criminals to obtain confidential information from the organizations' internal databases. Transportation schedules, blueprints of security systems and personnel information would enable the criminals, for example, to identify most attractive targets, plan optimal modus operandi and solicit key employees. Terrorists and criminals could take control of computer systems in a Trojan horse attack and thereafter shut down security systems or disrupt critical logistics services, such as an air traffic control system. Criminals often exploit the Internet as a channel to market illegal goods and services. E-mail and instant messengers helps the criminals plan and coordinate their operations conveniently and stealthily (Table 2).

The scenarios that were selected to provide a more detailed understanding of how cyber threats can be used to attack the supply chain or facilitate cargo crime are the following:

Table 2: How does cybercrime support offline supply chain crime?

Cybercrime objective / *Offline criminal activity*	*Access to confidential information*	*Control over computer systems*	*Communication*
Cargo crime	Logistics information: routing of shipments, content of shipments, scheduling etc. Vulnerability information: weak spots in security systems of terminals, ports and warehouses, etc.	Shut down or dislocation of surveillance cameras Manipulation of access control system	Coordination and planning within and between criminal groups Marketing transportation services via bogus websites set up for cargo crime purposes Web-sales and marketing of illegal goods
Smuggling	Vulnerability information: weak spots in anti-smuggling controls	Manipulation of shipment targeting results	Coordination and planning within and between criminal groups
Counterfeiting	Blueprints of genuine products Theft of serial numbers of products (spare parts, pharmaceuticals etc.)	-	-
Sabotage	Vulnerability information: weak spots in security systems of terminals, ports and warehouses etc.	Malicious tampering of supply chain related computer systems such as air traffic control, rail way control system, ERP-systems of businesses	Intimidation and blackmailing via internet Coordination and planning within and between criminal groups

- *Scenario 1*. Weapon Trafficking in maritime containers
- *Scenario 2*. Pharma Sabotage
- *Scenario 3*. Cargo Theft.

Scenario 1: Weapon Trafficking in maritime containers

Weapon trafficking also known as "gunrunning" or "arms smuggling" can be defined as the smuggling of weapons or arms across national borders. Even though the arms trafficking has been carried out across border countries using such methods for decades, it is quite obvious that the criminals are looking for more innovative methods; one of these could concern the exploitation of IT security weaknesses of logistics companies. For instance, criminal organizations might think that it is safer to use an established logistics company to support weapons smuggling across borders, since these companies can be subject to fewer inspections, while enjoying expedited control schemes. Hacking techniques such as phishing and key-logging could be used by hackers to access customs administrations' or supply chain companies' IT systems to target pre-cleared containers. Thereafter, by means of insiders the weapons are introduced in the containers and delivered to final destination without the risk of physical inspections.

Scenario 2: Pharma Sabotage

In this scenario we consider the threat of using a Stuxnet or Duqu-like virus to infect industrial machines of a pharmaceutical manufacturing company producing and delivering medicines to Europe. In particular, a virus (e.g. Duqu) could be used by hackers to start collecting information about 1) the ingredients used to manufacture a specific medicine and 2) the quality controls performed in the production, storage and distribution facilities of the pharma supply chain. After say months of gathering data, the hackers, in collaboration with a terrorist group and corrupted pharma experts, could attack the supply chain by changing the mix of ingredients and producing a mortal medicine. In addition, assuming that thresholds and quality control mechanisms are stored in electronic format, hackers could have the possibility to alter the detection mechanisms used to alert inspectors. After few months, the medicines will be distributed to Europe leading to a wave of death and health injuries that will continue until the authorities will discover the originating source and retire all the dangerous products from the market.

Scenario 3: Cargo Theft

Cargo crime, defined here as theft of cargo from commercial supply chains or exploitation of such supply chains to traffic stolen goods,[v] is a major concern for companies and authorities largely for financial, reputational and employee safety reasons.[34,35] Many cargo crime groups rely on accurate logistics information as they commonly accept assignments from external customers and operate on a *steal to order* basis.[36] Cargo thieves could use cybercrime tactics such as sniffing or phishing to get access to confidential information regarding contents, schedules and routes of shipments, helping them to identify shipments to steal. Likewise, documents may be altered to either add or remove information from shipping manifests. Infiltration into data systems of supply chain operators may also reveal security-sensitive information making cargo thieves capable of circumventing burglar alarms, cameras and other anti-theft measures. The company's own CCTV (Closed Circuit Television) systems could be exploited for spying and planning the theft. Likewise, fraudulent documentation could be stolen and reproduced by the criminals to facilitate the attack. After the attack, the hackers could cover theft of cargo by altering or deleting digital shipping documentation or warehouse records.

Discussion & Conclusion

The purpose of this paper is to enhance the understanding about how cyber threats may be exploited to perpetrate supply chain crimes. By means of a literature review, internal workshops and validation with three experts, this study develops three scenarios: weapons trafficking in maritime containers, pharma sabotage and cargo theft. The first scenario considers the hypothesis that weapons smuggling into sea containers could be facilitated by 1) accessing the IT systems of customs administrations or supply chain companies and 2) targeting those shipments that have been pre-cleared. The second scenario concerns stealing information about ingredients of pharmaceuticals and quality controls. The information is subsequently used by terror groups to alter the medicine and produce a mortal drug. The final scenario regards performing theft of cargo by accessing the information and ICT infrastructure to steal or alter information. The experts' validation confirmed the reality degree of the scenarios and most of all that vulnerability really exists.

In conclusion, it seems that IT vulnerabilities could be exploited by criminals to perpetrate their attacks and thereafter harm our communities. Huge amount of information is being stored by supply chain companies in electronic format. If criminals gain access to it, they will have the possibility to target shipments, people in the compa-

[v] Cross-border Research Association (CBRA) definition.

nies, and also to alter documentation to facilitate their illicit activities, e.g. smuggling, counterfeiting, sabotage, etc. Consequences of these attacks involve both the private sector and societal safety and may be extremely severe, especially if the attacks concern critical supplies to Europe, e.g. oil, minerals, rare earths, pharmaceuticals and food.

The European Union is actively working to raise attention on the cybersecurity topic and protection of ICT infrastructure. Despite the advanced and promising initiatives, there is still too scarce attention given to the vulnerability of supply chains against cyber threats. Much of the attention is being given to the protection of the public ICT infrastructure in Europe. However, this paper demonstrates that a terror attack might originate within a supply chain, with suppliers located outside the EU. This potential threat is under serious examination by the Department of Homeland Security (DHS) in the US. The fear of DHS is that cyber threats to US, e.g. viruses, could be hidden in computers, mobile phones or other IT equipment, delivered by high tech supply chains to the public administrations.[37] Therefore we suggest that more attention is equally given in Europe. In particular, we suggest that more research and initiatives concerning supply chain security and cybercrime are developed to enhance the protection of supply chains' information layers.

From a scientific viewpoint this paper discusses security concerns that are new to the supply chain literature. Hence, IT and supply chain managers are advised to consider these threats and take necessary actions. Finally, we discuss recommendations for the EU to support supply chain operators willing to mitigate cyber crime and cyber terrorism risks.

The main limitation of this study is that the development and validation of the scenarios has been performed with very few companies, with obvious issues concerning the generalization of the findings. Hence, our main recommendation is that any future research building upon this study should aim to increase the number of experts to be involved in the validation process.

Acknowledgement: The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 261633 (FOCUS project, www.focusproject.eu). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained therein.

Notes:

[1] Sarah Gordon and Richard Ford, "On the definition and classification of cyber crime," *Journal in Computer Virology* 2:1 (2006): 13-20.

[2] Symantec, "Internet Security Threat Report," *2011 trends*, vol. 17 (2011), www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf (7 Dec. 2012).

[3] Sophos, "Security threat report 2013," www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf?id=ee65b697-1d30-4971-b240-ce96b5e529aa&dl=true (7 Dec. 2012).

[4] Cisco, "Security Annual Report," www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf (7 Dec. 2012).

[5] UNODC, *World Drug Report 2011* (Vienna: United Nations Office on Drugs and Crime, 2011), www.unodc.org/documents/data-and-analysis/WDR2011/World_Drug_Report_2011_ebook.pdf (6 June 2012).

[6] Wendy Robson, *Strategic Management and Information Systems: An Integrated Approach*, Second edition (Essex, UK: Pearson Education Ltd., 1994).

[7] Alizera Bolhari, "Electronic-Supply Chain Information Security: A Framework for Information," paper presented at the 7th Australian Information Security Management Conference, Perth, Western Australia, 1-3 December 2009, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1009&context=ism (7 Dec. 2012).

[8] "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually," Press Release (Mountain View, CA: Symantec Corp., 7 Sep. 2011), www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (6 June 2012).

[9] Ponemon Institute, "Second Annual Cost of Cyber Crime Study," August 2011, www.securitymanagement.com/article/cost-cybercrime-009154 (6 June 2012).

[10] MSB, *Measures to improve Sweden's ability to prevent and handle IT incidents*, Report on the government assignment to the Swedish Civil Contingencies Agency MSB 0163-10, Fö2009/2162/SSK, 13 Jan. 2010, www.msb.se/RibData/Filer/pdf/25903.pdf (6 Dec. 2012).

[11] European Network and Information Security Agency (ENISA), *France Country Report*, May 2011, www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/France.pdf (7 Dec. 2012).

[12] John Joseph Coyle, C. John Langley, Brian J. Gibson, Robert A. Novack, and Edward J. Bardi, *Supply Chain Management: A Logistics Perspective*, Eight edition (Mason, OH: South Western Cengage Lerning, 2009).

[13] Matthew Warren and William Hutchinson, "Cyber Attacks Against Supply Chain Management Systems: A Short Note," *International Journal of Physical Distribution & Logistics Management* 30:7-8 (2000): 710–16.

[14] Lisa R. Williams, Terry L. Esper, and John Ozment, "The Electronic Supply Chain: Its Impact on the Current and Future Structure of Strategic Alliances, Partnerships and Logistics Leadership," *International Journal of Physical Distribution & Logistics Management* 32:8 (2002): 703–19.

[15] Zeviar-Geese Gabriole, "The State of the Law on Cyber Jurisdiction and Cybercrime on the Internet," *Gonzaga Journal of International Law* 1 (1997-1998).

[16] *The United Nations Manual on the Prevention and Control of Computer Related Crime*, supra note 41, paragraphs 20 to 73 in International Review of Criminal Policy (1995): 43–44, www.uncjin.org/Documents/EighthCongress.html.

[17] Omera Khan and Adrian Davis, "Managing Cyber and Information Risk," paper presented at the 17th Annual Logistics Research Network Conference, Cranfield, UK, 5-7 September 2012.

[18] Earl R. Babbie, *The Practice of Social Research*, Twelfth edition (Belmont, CA: Wadsworth Cengage Learning, 2010).

[19] "The Stuxnet Outbreak, A Worm in the Centrifuge – An Unusually Sophisticated Cyber-weapon is Mysterious but Important," *Economist*, 30 September 2010, www.economist.com/node/17147818.

[20] Kevin McCaney, "Was double agent responsible for Stuxnet attack on Iran?" *Defence Systems*, 17 April 2012, http://defensesystems.com/articles/2012/04/13/stuxnet-planted-by-iranian-double-agent-israel.aspx?admgarea=DS (7 Dec. 2012).

[21] John Markoff and David E. Sanger, "In a Computer Worm, a Possible Biblical Clue," *The New York Times*, 29 September 2010, www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=1&_r=4&hpw (21 July 2012).

[22] Lee Ferran and Rhonda Schwartz, "Cyber Spy Program Flame Compromises Key Microsoft Security System," *ABC News*, 4 June 2012, http://abcnews.go.com/Blotter/cyber-spy-program-flame-compromises-key-microsoft-security/story?id=16492180#.UOmjrvUrnIU (7 Dec. 2012).

[23] Luca Urciuoli, *Security in Physical Distribution Networks: A Survey of Swedish Transport Operators*, PhD thesis (Lund, Sweden: Lund University, 2011). ISBN 978-91-976974-5-3, http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1761619&fileOId=1761630 (7 Dec. 2012).

[24] Juha Hintsa, *Post-2001 Supply Chain Security – Impacts on the Private Sector*, Doctoral Thesis dissertation (Lausanne, Switzerland: Université de Lausanne, 2011).

[25] Toni Männistö, *Supply Chain Security – Disclosing User's Requirements*, Master's thesis (Helsinki: Aalto University School of Science and Technology, 2011)

[26] *Development of a Strategic Roadmap Towards a Large Scale Demonstration Project in European Logistics and Supply Chain Security*, LOGSEC Deliverable, 31 March 2011, www.logsec.org/images/upload/file/docs_logsec-roadmap-finalpublic.pdf (6 June 2012).

[27] *Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles*, FOCUS Deliverable 5.1, www.focusproject.eu/web/focus/ downloads/-/document_library_display/1QpQ/view/15032/732?_110_INSTANCE_1QpQ_redirect=http%3A%2F%2Fwww.focusproject.eu%2Fweb%2Ffocus%2Fdownloads%2F-%2Fdocument_library_display%2F1QpQ%2Fview%2F15032 (6 Dec. 2012).

[28] *Managing Emerging Threats in ICT Infrastructures*, White Book, Forward Deliverable 3.1, www.ict-forward.eu/media/publications/forward-whitebook.pdf (22 Nov. 2012).

[29] *Initial Analysis of the Industrial Case Studies*, Aniketos Deliverable 6.1, 19 July 2011, www.aniketos.eu/sites/default/files/downloads/Aniketos%20D6.1%20Initial%20analysis%20of%20the%20industrial%20case%20studies.pdf (6 Dec. 2012).

[30] *Second Report on Threats on the Future Internet and Research Roadmap*, SySSec Deliverable 4.2, www.syssec-project.eu/media/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf (6 Dec. 2012).

[31] *Trustworthy Clouds, Privacy and Resilience for Internet-scale Critical Infrastructure* (Tclouds), www.tclouds.eu (6 Dec. 2012).

[32] Zachary Williams, Jason E. Lueg, and Stephen A. LeMay, "Supply Chain Security: An Overview and Research Agenda," *The International Journal of Logistics Management* 19:2 (2008): 254–81.

[33] *Transportation & Logistics 2030*, Volume 4: *Securing the Supply Chain*, Pricewaterhouse Coopers, www.pwc.com/gx/en/transportation-logistics/publications/security-transport-systems.jhtml.

[34] International Road Transport Union, *Attacks on Drivers of International Heavy Goods Vehicles: Facts and Figures* (2006), www.iru.org/cms-filesystem-action?file=webnews2008/Attack%20survey%20exec.summ%20-%20EN.pdf (17 April 2012).

[35] Transported Assets Protection Association (TAPA), www.tapaemea.com.

[36] *National Threat Assessment 2008. Organised Crime* (Zoetermeer, The Netherlands: KLPD–IPOL Department, Netherlands Police Agency, April 2009), www.csd.bg/fileadmin/user_upload/Countries/Netherlands/Dutch%20National%20%20threat%20assessment%202008_tcm35-504488.pdf (17 April 2012).

[37] "Homeland Security chief contemplating proactive actions against cyber attacks," *Mercury News*, 16 April 2012, www.mercurynews.com/business/ci_20410915/homeland-security-chief-contemplating-proactive-cyber-attacks?source=rss (17 April 2012).

LUCA URCIUOLI, PhD, holds a Master of Science degree in Industrial Engineering from Chalmers University of Technology, Gothenburg, and a Doctorate in transportation security from the Engineering University of Lund, Sweden. He has been working at the research unit of the Volvo group as a project manager developing telematics services in the areas of transport and logistics optimization, security, and up-time management and diagnostics. At the University of Lund he has been responsible for the course in International physical distribution and has published diverse transport safety and security articles in conference proceedings and scientific journals. Since 2010, Dr. Urciuoli works as the research director of Cross-border Research Association (CBRA). Mailing address: Cross-border Research Association, Route de la Chocolatière 26, 1026 Echandens, Switzerland. *E-mail:* luca@cross-border.org

TONI MÄNNISTÖ is a PhD candidate at École Polytechnique Fédérale de Lausanne (EPFL) where his PhD research focuses on security of global supply chains. He obtained his MSc degree in Industrial Engineering and Management from Aalto University School of Science and Technology in Helsinki in 2011. During his studies, Toni expanded his professional expertise by working for several organizations including his current employer, Cross-border Research Association. He has worked in projects dealing with customs risk management, catastrophe logistics, tracking technologies in postal supply chains, distribution of pharmaceuticals and supply chain security. *E-mail:* toni@cross-border.org

JUHA HINTSA, PhD, is the founder and director of Cross-border Research Association (CBRA), and a collaborator with HEC Université de Lausanne, Department of Operations, from where he holds a doctorate of management degree. He specializes in supply chain security research. He has some 40 journal and conference publications and book contributions, and is a regular speaker and guest lecturer at related events worldwide. He is active in multiple European research and standardisation projects, including Framework Program 7 (FP7) and European Committee for Standardisation (CEN). Dr. Hintsa is also a member of TAPA EMEA regulatory affairs working group; PICARD advisory group for the World Customs Organization (WCO); and editorial board member for the Journal of Transport Security and the World Customs Journal. *E-mail:* juha@cross-border.org

TAMANNA KHAN has obtained her MSc degree in Management from HEC, University of Lausanne and a bachelor degree in Industrial Engineering from the University of Texas at Arlington. She has been working as a researcher in supply chain security with her current employer Cross-border Research Association since 2007. She was involved in Supply Chain Security Management projects financed by the Swiss National Foundation (SNF), creating case studies and cross-analysis of corporate logistics and security guidelines versus a European supply chain security standard requirements (EU AEO), and took part in the local and global supply chain security standards for cross-analysis in the FP7 funded China-EU secure trade lane project INTEGRITY. *E-mail:* tamannat.khan@gmail.com