CRITICAL ENERGY INFRASTRUCTURE AT RISK OF CYBER ATTACK

Frank Umbach

At the end of May, a new super worm called Flame was discovered that seems to be even more intricate and complex than the Stuxnet sabotage worm that was identified in the summer of 2010.[1] Both these worms targeted Iran and its nuclear installations, though Flame is primarily an across-the-board espionage programme. At the same time there have been increasing signs that the Stuxnet worm, designed to attack supervisory control and data acquisition systems configured to monitor industrial processes using the code word "Olympic Games", was in fact created by the USA in collaboration with Israel.[2] Of course, the identification and "exposure" of the creator of the Stuxnet worm has brought with it a significant amount of political fall-out[3] – particularly in view of the ongoing negotiations between the international community and the USA with Iran, a country suspected of developing a nuclear weapons programme. In the long-term the USA could even be the biggest loser, as malware such as Stuxnet and Flame can often be copied, modified and enhanced by their targets

Dr. Frank Umbach is Associate Director of the European Centre for Energy and Resource Security (EUCERS) at King's College in London, Head of the "International Energy Security" programme at the Centre for European Security Strategies (CESS GmbH) in Munich and Non-Resident Senior Fellow of the U.S. Atlantic Council in Washington D.C.

1 | Cf. David E. Sanger, "Obama Stepped up Wave of Cyberattacks on Iran", *The New York Times*, 1 Jun 2012; Nicole Perlroth, "Researchers Find Clues in Malware", *The New York Times*, 30 May 2012; Michael Borgstede, "Ein Virus nach dem Baukastenprinzip", *Die Welt*, 30 May 2012, 6; "'Der Feind am Ende der Leitung hört mit' – Interview mit Alexander Gostew, Chef-Experte des Antiviren-Unternehmens Kaspersky Lab", *Die Welt*, 30 May 2012, 10; Thomas Erdbrink, "Iran Confirms Attack by Virus That Collects Information", *The New York Times*, 29 May 2012.

2 | Cf. Ansgar Graw, "Barack Obama führt den Krieg der Zukunft", *Die Welt*, 3-6 Jun 2012, 4; idem, "US-Präsident befahl Angriff mit Stuxnet-Virus", *Die Welt*, 2 Jun 2012.

3 | Cf. Sandro Gaycken, "Strategische Kollateralschäden", *Handelsblatt*, 6 Jun 2012.

and other third parties. Today the USA certainly possesses the most potential for inflicting cyber attacks, but at the same time, its high-tech industrial society is so reliant on IT that it is extremely vulnerable if its defence capabilities lag behind its ability to attack. Has the USA opened Pandora's box by unleashing the Stuxnet worm?

CRITICAL NATIONAL INFRASTRUCTURES AT RISK

The discovery of this digital malware is particularly explosive because it makes it clear that the development and use of cyber weapons by nation states for use against industrial targets and therefore also against critical infrastructures is much more advanced than experts believed prior to 2010. According to former anti-terrorism advisor Richard Clarke, between 20 and 30 states have the capability to launch cyber warfare.[4] These include not only the USA, China and Russia, but also smaller states and numerous medium-sized powers, including Iran and North Korea. Since 2011, groups of Israeli and Arab hackers have been waging a new kind of undeclared war with escalating cyber attacks and constant "retaliatory strikes".[5]

Between 20 and 30 states have the capability to launch cyber warfare. These include not only the USA, China and Russia, but also smaller states and numerous medium-sized powers, including Iran and North Korea.

Over recent years, cyber attacks and cybercrime have become a massive threat to industry and governments alike. They have caused worldwide losses amounting to hundreds of billions of euros. In Germany, the Bundeskriminalamt (Federal Criminal Police Office) estimates that cyber criminals caused losses of 71 million euros in 2011, but the real figure is much higher.[6] There are often close ties between individuals and government authorities in this area. The Russian Business Network (RBN) is known around the world as one of the most powerful and dangerous cybercrime organisations. It is the only cybercrime organisation that NATO has rated as a major threat. Allegedly, this

4 | Cf. Richard A. Clarke and Rob Knake, *World Wide War. Angriff aus dem Internet*, Hoffmann und Campe, Mar 2011.

5 | Cf. Max Borowski, "Cyberschlacht im Nahen Osten", *Financial Times Deutschland*, 11 Jan 2012, 11; Tom Gara, "Uprisings Spark an Increase in Malicious Activity Online", *Financial Times*, 27 Mar 2012, 1.

6 | Cf. Annika Graf, "Unternehmen erschweren Schutz vor Hacker-Attacken", *Financial Times Deutschland*, 31 May 2012, 3; Hans Evert, "Unternehmen im Netz der Wirtschaftspione", *Die Welt*, 4 Apr 2012, 12.

organisation is responsible for 40 per cent of the world's cybercrime, amounting to over 100 million U.S. dollars in 2007 alone.[7] These kinds of cyber attacks are a threat to everything we do, as the world is increasingly dependent on information technology and the internet in all areas of life.[8]

Cyber attacks are a threat to everything we do, as the world is increasingly dependent on information technology and the internet in all areas of life.

It is not only private individuals and companies that are affected by the theft of their personal customer data or sensitive operational information. Increasingly, governments find themselves under threat, along with their communication channels and infrastructures. In early 2011 Canada and France were hit particularly hard by cyber attacks, but almost every Western state has been and is being affected by such attacks. Often it is not just a case of data theft, but of distributed denial of service (DDS), where servers are bombarded by so many requests that they collapse and can no longer be accessed by their customers. These kinds of cyber attacks are then only halted upon payment of a "ransom".[9]

Not just individual hackers or loosely-organised political groups such as Anonymous or Lulzsec who behind the attacks, it can also be hostile governments who hide behind "unholy alliances" with criminal syndicates, terrorists or nationalist movements or people, without running any risk of being discovered or identified. Security experts consider "critical infrastructures" to be at particular risk, as these are essential for a state's survival and to sustain vital state functions. Critical infrastructures include information systems, telecommunications, the transport and traffic sectors, energy supply, healthcare, financial services and

7 | Cf. Newsweek (ed.), "The (Evil) Cyber Empire", 29 Dec 2009; Alexander Klimburg, "Mobilising Cyber Power", *Survival*, Mar-Apr 2011, 41-60, here: 48 et sqq.

8 | Cf. also Sandro Gaycken, C*yberwar. Das Internet als Kriegsschauplatz*, Munich, 2011.

9 | Cf. also Misha Glenny, *Cybercrime. Kriminalität und Krieg im digitalen Zeitalter*, Munich, 2012.

other sensitive services.[10] These critical infrastructures are all characterised by their high levels of internal complexity and dependency, as well as by their vulnerability. But at the same time specific responsibilities, laws and regulations vary widely amongst the 27 EU member states. Within each country, these are divided among federal state structures, such as the federal and state levels in Germany, and between various ministries. On top of this, in both Germany and Europe as a whole, 80 per cent of critical infrastructures are in the hands of private companies. This requires ongoing cooperation between government departments and the private sector. However, until just a few years ago, this was not institutionalised in most EU countries, and the responsibilities of state and private sector were not clearly and jointly regulated.

In both Germany and Europe as a whole, 80 per cent of critical infrastructures are in the hands of private companies. This requires ongoing cooperation between government departments and the private sector.

The need to protect critical infrastructures as a potential national and international security risk was identified back in the mid-1990s, but it has only been taken seriously since 2001, as a result of international terrorism and the creation of the U.S. Department of Homeland Security. In recent years, the focus of security concerns has shifted from physical terror attacks to cyber attacks. Since the terror attacks of 11 September 2001, critical infrastructures have increasingly been the target of cyber attacks. In 2009, viruses were discovered in the U.S. electricity grid that supposedly originated from China and Russia and which could have made the USA a victim of blackmail if relations between the two countries were to sour.

10 | Cf. "Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection", 2008/114/EC, Brussels, 8 Dec 2008; "Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure", research project funded by European Union/DG Justice, Freedom and Security, Final Report, 2009; Federal Ministry of the Interior (BMI), "Protecting Critical Infrastructures – Risk and Crisis Management", Berlin, Jan 2008. See also the websites of the commision: "Energy Infrastructure: Critical Infrastructure Protection", http://ec.europa.eu/energy/infrastructure/critical_en.htm (accessed 23 Jul 2012); "Critical Information Infrastructure Protection", http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm (accessed 23 Jul 2012); "European Programme for Critical Infrastructure Protection (EPCIP)", http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm (accessed 23 Jul 2012).

Damage or disruption to sensitive operational and communications processes within and between critical infrastructures could lead to extensive political, social and economic fall-out that could also quickly spill over into other (neighbouring) states.[11] All critical infrastructures in modern industrial societies are increasingly integrated and inter-linked by two things: electricity and the internet. Any longer-term disruption to electricity and/or the internet would mean that a country could lose essential services such as energy and water supply and thus could no longer guarantee the functioning of its critical infrastructures.[12] The more an industrialised society and its critical infrastructures are linked by the internet, the greater its vulnerability and the potential risks it faces.[13]

Longer-term disruption to electricity and the internet would mean that a country could lose essential services such as energy and water supply and hence could no longer guarantee the functioning of its critical infrastructures.

Western security experts believe cyber attacks are the greatest threat to European energy supplies and to critical energy infrastructures. Critical energy infrastructures particularly include installations and networks for generating electricity, but also for the extraction of oil and gas, storage and refineries, liquid gas terminals, as well as transport and distribution systems. Energy control centres are particularly sensitive and vulnerable with their SCADA systems for monitoring and controlling energy supplies.[14]

11 | Cf. also Commission of the European Communities, "Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience", SEC(2009) 399/SEC(2009)400, Brussels, 30 Mar 2009, COM(2009)149 final; Frank Umbach, "Waking Up to Cyber-Attack Threats in All Walks of Life", Special Report, *Geopolitical Information Service*, 13 Oct 2011, 4.

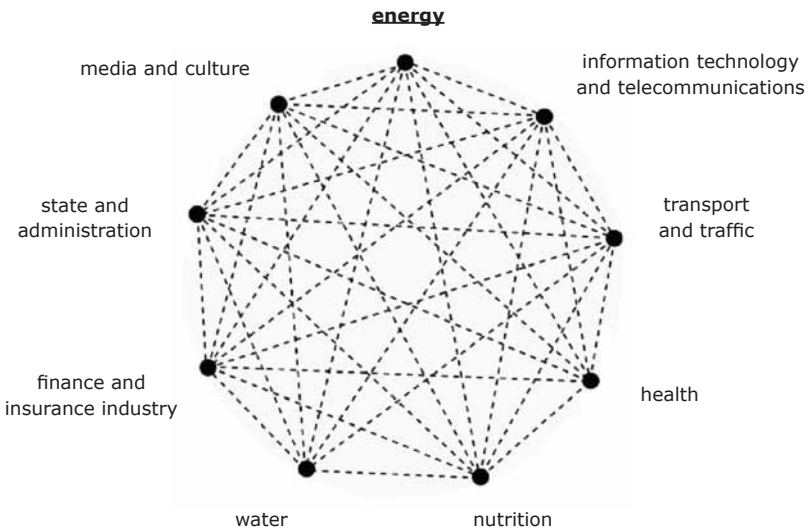
12 | Cf. also Frank Umbach, "Europe's New Electricity Networks Face Danger of Cyber-Attacks", Special Report, *Geopolitical Information Service*, 18 Oct 2011.

13 | Cf. n. 11.

14 | Cf. also Frank Umbach and Uwe Nerlich, "Asset Criticality in European Gas Pipeline Systems – Increasing Challenges for NATO, its Member States and Industrial Protection of Critical Energy Infrastructure", in: Adrian Gheorghe and Liviu Muresan (eds.), "Energy Security. International and Local Issues, Theoretical Perspectives and Critical Energy Infrastructures", *NATO Science for Peace and Security Series – C: Environmental Security*, Springer, Dordrecht, 2011, 273-303; Frank Umbach, "Critical Energy Infrastructure Protection in the Electricity and Gas Industries. Coping with Cyber Threats to Energy Control Centers", *OSCE-CTN Newsletter*, Special Bulletin: "Protecting Critical Energy Infrastructure from Terrorist Attacks", Vienna, Jan 2010, 25-28.

Although the increase in cyber attacks has generally led Western governments and industrial enterprises to take the issue of security more seriously over recent years, they have failed to keep pace with the new threats that make them so vulnerable in cyberspace. This lack of security consciousness can affect every area of private and public life, domestic and international trade and even the defence policy of countries and multinational organisations such as the European Union and NATO.

Fig. 1
Interdependencies between critical infrastructures



Source: German Federal Ministry of the Interior, *Protection of Critical Infrastructures. Risk and Crisis Management. Guidelines for Companies and Authorities*, Berlin, May 2011, 10.

However, since 2005 the EU-27 have become increasingly aware of the potential dangers posed by such cyber attacks on critical infrastructures and developed corresponding domestic and multilateral counter-strategies. But these strategies have still not been adequately implemented at national and EU level. For reasons of history and tradition, each country favours their own security concepts, institutions and programmes as a means of reacting effectively to the new security threats to their critical infrastructures including the critical information infrastructure/CII. But

national security measures on their own are not enough, as these types of cyber attacks have reached new levels of sophistication and the vulnerability of digital systems and networks have grown exponentially over the last few years. The damage caused by cybercrime and cyber espionage has reached frightening proportions, particularly in Western countries, because the technical measures they have taken and the laws and regulations they have passed are always lagging behind the cyber criminals.

Table 1
Milestones of the EU's Critical Infrastructure Protection (CIP) Programme

2005	Green Paper on a European Programme for Critical Infrastructure Protection
2006	European Programme for Critical Infrastructure Protection (EPCIP)
2008	EU Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection
2009	Communication on Critical Information Infrastructure Protection
May 2010	Adopting the Digital Agenda, which sets out security as a prerequisite for ICT take-up
September 2010	EC adopts proposal for a Directive
September 2010	EC-Proposal to strengthen ENISA
November 2010	Establishment of the EU-US Working Group on Cyber Security and Cyber-crime
March 2011	EC-Communication on Critical Information Infrastructure Protection (CIIP) „Achievements and Next Steps: Towards Global Cybersecurity"
End 2011	Joint EU-US Cyber-incident exercise
2013	ENISA will begin operation of a European Information Sharing and Alert System (EISAS)

Source: *EurActive*.

In the ancient battle between attackers and defenders, now more than ever the attackers seem to have the advantage. They are better equipped, can choose the intensity and targets of their attacks and are no longer hindered by geographical distance or national borders. The attacker can

also operate in secret, generally remains anonymous and has the chance to select efficient and "cheap" asymmetric strategies.

All of these new cyber threats to critical national infrastructures have created worldwide demand for modern security technologies, services and management capabilities. The market for civil defence products and services and for ICT and software manufacturers to protect against terrorists, pirates, criminals and hackers is the world's fastest-growing sector. The global network security market alone is estimated to have grown to 60 billion U.S. dollars and over the next 3 to 5 years it is expected to see an average increase of 10 per cent per annum.[15]

A DIGITAL PEARL HARBOUR? NEW SECURITY RISKS AND VULNERABILITY TO CYBER ATTACK OF CRITICAL INFRASTRUCTURES[16]

Cyber attacks can be carried out using malware in the form of viruses, worms, Trojans and DDS attacks by individuals or by criminal or terrorist organisations. They are used for espionage purposes and to disrupt and damage the control, monitoring, information and communication processes of critical infrastructures and companies. However, most cyber attacks are still aimed at spying on or stealing sensitive customer data or industrial secrets. One of the first cases of cyber warfare occurred as early as 1982, when a Canadian firm's computer operating system was stolen by the Soviet secret services and later resulted in an explosion in a Soviet oil pipeline. The software code had previously been tampered by the CIA in order to create a "logic bomb".[17]

15 | Cf. "Kalter Krieg im Internet", *Die Welt*, 4 May 2012, 14.

16 | The following analysis is also based on the results of major European Commission research projects (Octavio, Inspire) in recent years in which the author and CESS GmbH in Munich were involved. Cf. "Octavio: Energy System Control Centers Security – an EU Approach", research project funded by European Union/DG Justice, Freedom and Security under Program C 2008/60/03: Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks, *Final Report 2009*; *Inspire: Increasing Security and Protection Through Infrastructure Resilience*, research project funded by European Union under 7th FWP (Seventh Framework Program), 31 Oct 2010.

17 | David J. Betz and Tim Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power*, Adelphi Series IISS, No. 424, London-Abindon-Oxon, 2011, 20 et seq.

The attackers can activate viruses at any time and in any place around the world through a computer in the computer network and paralyze servers and websites through DDS attacks.

The situation has become even more dangerous with the creation of botnets via infected computers. These are used for criminal purposes and can insert Trojans that are invisible to the internet user. The attackers can activate these viruses at any time and in any place around the world through a computer in this computer network and paralyse servers and websites through DDS attacks. They allow criminals and terrorists to carry out massive attacks through stealing and falsifying data or through destroying, altering or manipulating confidential data with hugely damaging consequences for industry and other critical national infrastructures. The most dangerous botnet threat at the present time is Conficker, which has infected more than 1.5 million computers around the world and has the potential to take over and control another 5 million computers in 122 countries. Even though this worm has so far not been "awoken" and activated, its origin is still unknown and no counter-strategies have been developed.[18] With this in mind, Henning Wegener, Chairman of the Permanent Monitoring Panel on Information Security at the World Federation of Scientists, warned in 2009: "The vulnerability of digital terminals and the networks that connect them has been underestimated – despite the fact that the risks and losses are growing alarmingly and exponentially as attacks escalate and become increasingly sophisticated. The dynamics of this growth, the uncontrolled proliferation of attacks in cyberspace and the enormous exponential growth in the risks show that we are facing a quantum leap in terms of digital threats."[19]

The first more major and well-coordinated cyber attack with state involvement was carried out in the course of the diplomatic disputes between Russia and Estonia in 2007-2008 and between Russia and Lithuania in 2008, when Estonian and Lithuanian governmental and communications networks were temporarily disabled. Similarly, before and during the military conflict between Russia and Georgia in summer 2008, Georgian governmental functions and other important communications structures were successfully

18 | Cf. also Mark Bowden, *Worm. Der erste digitale Weltkrieg*, Berlin, 2012.

19 | Henning Wegener, "Der unsichtbare Feind. Die neuen Gefahrenlagen im digitalen Raum", *Internationale Politik*, Sep-Oct 2009, 48-57, here: 48.

attacked and long-term damage was inflicted, including the shutting down and malicious takeover of the Baku-Tbilisi-Cehnan oil pipeline. But despite all the evidence and indications, it was impossible for Estonia, Georgia, NATO and the EU to prove that the attacks came from Russia.[20] In July 2009 more than 12,000 computers in South Korea and a further 8,000 in the USA and other countries were attacked from North Korea, but again it was impossible to prove who was responsible.

In July 2009 more than 12,000 computers in South Korea and a further 8,000 in the USA and other countries were attacked from North Korea, but again it was impossible to prove who was responsible.

The huge increase in private and state-sponsored cyber attacks by individual hackers, loose political groups, international organised crime, terrorist cells and governmental institutions (such as the secret services, foreign armed forces, etc.) can be explained by the following factors:

- Currently it can be proven which country is the originator of a cyber attack, but not to pinpoint exactly who is responsible. In certain circumstances it is possible for a computer within a particular country to be used by groups from outside that country. As long as the international community is unable to clearly prove who is responsible for these kinds of attacks, the attackers feel safer than ever and every year their numbers increase, as is shown by international cybercrime statistics. In future it is likely that well-organised international organised crime syndicates will not only have an interest in stealing customer data but will increasingly turn their attention to industrial espionage and blackmail.

- The countless new security risks are the result of the spread of information and communications technology (ICT), which will continue to increase dramatically over the coming years in line with the growth in the worldwide flood of information. This will mean that information and communications structures will become even more closely linked, resulting in additional security risks.

20 | Cf. Bruce Averill and Eric A.M. Luiijf, "Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention", *Journal of Energy Security*, 18 May 2010, 1, http://ensec.org/index.php?option=com_content&view=article&id=243 (accessed 24 Jul 2012).

- Market liberalisation and the privatisation of formerly state-run infrastructure operators, along with new regulations, have made the private sector and government agencies ever more dependent on external providers of goods and services. In parallel to this, financial and competitive pressures have resulted in the development of specific software exclusively for industry to be discontinued in favour of commercial off-the-shelf (COTS) products.

- Almost every individual service is directly or indirectly dependent on a secure power supply. The size and complexity of the physical, virtual and logical networks has soared. A result of the growing mutual dependency between different critical infrastructures, the dependency and consequences of supply bottlenecks and disruptions is generally not obvious as long as a crisis does not hit causing a total collapse in supply. However, even smaller power fluctuations, outages and interruptions can have dramatic effects that cannot always be predicted as systems become ever more complex.

- The all-pervasiveness of the threat and the effectiveness of cyber attacks have become the new fifth front of warfare after land, water, air and space. They present a brand new challenge for the international community in a rapidly-changing global security landscape.[21] These threats are also increasingly calling into question traditional concepts and ideas of national and collective security and defence. The new era of cyber warfare can be compared with technological leaps in history such as the first use of gunpowder, the invention of the tank or the dropping of the first atomic bomb on Hiroshima.[22]

The risk of a "digital Pearl Harbor" in the 21st century has now become very real and can no longer be considered to be within the realm of science fiction, as the boundaries between cybercrime, cyber terrorism and cyber war waged by individuals or nation states as a new form of "asymmetric warfare" have become increasingly fluid. In 2008 the World Economic Forum warned that there was a 10-20 per cent

21 | Cf. aso Joachim Zeppelin, "Schutz im unsichtbaren Cyberkrieg", *Financial Times Deutschland*, 11 Jun 2012, 25.
22 | Clemens Wergin, "Der Krieg der Zukunft", *Die Welt*, 2 Jun 2012, 1.

U.S. experts have warned that a successful cyber attack on the American electrical power supply could cost the economy 700 billion U.S. dollars, comparing it to the effect of 40 or 50 huge hurricanes all striking simultaneously.

chance of a large-scale collapse of the CII in the next ten years and that this could cause damage to the world's economies amounting to 250 billion U.S. dollars.[23] Since then, U.S. experts have warned that a successful cyber attack on the American electrical power supply could cost the economy 700 billion U.S. dollars, comparing it to the effect of 40 or 50 huge hurricanes all striking simultaneously: "It's greater economic damage than any modern economy ever suffered. […] It's greater than the Great Depression. It's greater than the damage we did with strategic bombing on Germany during World War II."[24]

It has been proven that in May 2008 Russian hackers penetrated the nuclear power plant near Saint Petersburg. Although the operation of the plant was not affected, there were widespread rumours – possibly spread intentionally – that there had been a radioactive leak from the plant. Communications between the plant and the plant operator Rosatom were also cut for several hours.[25]

It is also worrying that in early 2010 and 2011 hackers struck the EU's Emissions Trading System (ETS), demonstrating once again the potential of cyber attacks to manipulate market prices and influence who can conclude energy contracts. Over 2 million certificates – though this figure only represented 0.02 per cent of all certificates – were transferred illegally to particular accounts during the attack in January 2011. Previously, the ETS had already been temporarily closed after 475,000 certificates were stolen when the Czech emissions register was hacked. Other platforms such as the France Bluenext Exchange were also forced to close. Austria, Poland, Estonia and Greece also blocked

23 | Cf. Commission of the European Communities, "Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience", SEC(2009)399/SEC(2009)400, Brussels, 30 Mar 2009, COM(2009)149 final, 2.

24 | Scott Borg, Chief Economist at U.S. Cyber Consequences Unit, a privat non-profit think tank, quoted in: J.N. Gordes and M. Myirea, "A New Security Paradigm Is Needed to Protect Critical US Energy Infrastructure from Cyberwarfare", *Foreign Policy Journal*, 14 Sep 2009.

25 | Cf. "How Vulnerable are Energy Facilities to Cyber Attacks", *Intelligence Report*, Securing America's Future Energy (SAFE), Washington D.C., Vol. 3, No. 1, 20. Jan 2010, 2, http://secure energy.org (accessed 23 Jul 2012); Averill and Luiijf, n. 19, 2.

their trading registers. The losses were put at over 5 billion euros. Even more problematic is the way the credibility of the ETS has been undermined in its role as Europe's most important instrument for reducing harmful emissions.[26]

Table 2

State-funded and sponsored cyber attacks

Estonia: April-May 2007
Lithuania: June-July 2008
Georgia: July-August 2008
South Korea and USA: in July 2009 (in South Korea 12,000 computers were attacked and 8,000 in other countries; the attack originated in North Korea)
United Kingdom 2006: caused the British Parliament's computer system to shut down; and 2007 attacks on the systems of the British Foreign Office and other major government departments.
India: attacks on ministries, telecommunications centres and companies, troops and military installations, embassies and consulates, encrypted diplomatic communications and the Secretariat of the National Security Council.
The Netherlands: DigiNotar, the private company used by the Dutch government to provide authentification certificates for government websites.
USA: the Pentagon computers are scanned 250,000 times an hour, up to 6 million times a day.
In 2010 NATO had to deal with hundreds of malicious cyber incidents on a daily basis.
April 2012: over 600,000 Apple computers – until then considered much more secure and less susceptible to attack than computers run on Windows software – were infected with the Flashback Trojan.

Manipulations such as these can also lead to interruptions in energy supplies and power cuts. The spot energy market and other energy trading platforms such as the Amsterdam Power Exchange/APX, Paris Powernext and the European Energy eXchange/EEX in Germany all operate via the regular internet and are hence exposed to the risk of external

26 | Cf. European Commission, "Emissions Trading: Q & As Following the Suspension of Transactions in National ETS Registries for at least One Week from 19:00CET on Wednesday 19 January 2011", Brussels, 21 Jan 2011; Michael Gassmann, "Emissionsstelle dichtet Sicherheitslecks ab", *Financial Times Deutschland*, 23 Feb 2010, 5; Averill and Luiijf, n. 19, 4.

manipulation.[27] This was shown in February 2011 when the Nasdaq Stock Exchange in New York also fell victim to a cyber attack, even though the hackers were not able to penetrate the trading system. However, these examples demonstrate very clearly the vulnerability of the stock exchanges, most of which are now totally computerised.[28]

Table 3
Selected recent cybercrime attacks

Angriffsziel	**Jahr**	
International Monetary Fund (IMF)	2011	Large-scale and well-planned attack on a database containing information that could influence the market, including confidential details of international aid.
Citigroup	2011	Hackers stole data on 200,000 borrowers, including addresses, passwords etc.
Dropbox	2011	A popular service for storing documents and other files in a computing cloud.
Comodo Group	2011	Internet security firm providing website authentication certificates for browsers operated by Google, Yahoo, Microsoft, Skype and Mozilla (over 676 organisations use Comodo for certifications).
Nasdaq Stock Exchange, New York	2011	Hacked, but the trading system was not breached.
Lockheed Martin	2010/2011	Industrial espionage (from China).
MasterCard, Visa und PayPal	2010	Anonymous, a loose group of hackers from all over the world declared cyber war on MasterCard, Visa and PayPal because they refused to pass on donations to Wikileaks.
Google	2009/2010	Google and 30 other high-tech companies in the USA.
Sony Webseite		Theft of personal information such as the passwords, e-mail addresses and postal addresses of more than 52,000 customers.
RSA Security	2010	Creates passwords for large companies to protect them from intruders.
Energy Industry, United Kingdom	2009	Night Dragon attacks on the energy industry causing losses of over 30 billion euros. They have reportedly been emanating from China since November 2009.

27 | Cf. Rowena Mason, "European Carbon Market Suspended over Frauds", *The Telegraph*, 19 Jan 2011.
28 | Cf. Graham Bowley, "Hackers Gained Access to Nasdaq Systems, but not Trades", *The New York Times*, 5 Feb 2011.

LESSONS FROM AMERICA – THE INTERNATIONAL DIMENSION

While the UK suffered financial losses amounting to 30 billion euros as a consequence of cyber attacks in 2009, according to President Barack Obama the USA lost as much as 1 billion U.S. dollars in the same year due to cybercrime. In the wake of this, the U.S. administration announced the launch of a 17-million dollar digital defence programme and named Howard A. Schmidt, an experienced computer specialist, as the White House's co-ordinator for cyber-security. 2009 also saw the establishment of the U.S. Cyber Command (USCYBERCOM) led by four-star general Keith Alexander. In July 2011 the U.S. Defense Department finally introduced its long-awaited "Strategy for Operating in Cyberspace" which warned that: "Our reliance on cyberspace stands in stark contrast to the inadequacy of our cyber-security."[29] Pentagon officials were also forced to admit that even their protected intranet, which is largely separate from regular internet, is not immune to cyber attacks.

Pentagon officials were forced to admit that their protected intranet, which is largely separate from regular internet, is not immune to cyber attacks.

The U.S. administration's defence programme against cyber attacks was largely a direct result of an attack on the world's best-known search engine, Google. Chinese hackers stole huge amounts of intellectual property and sensitive customer data from Google in what became known as Operation Aurora. But this attack on Google was only the tip of the iceberg, as was to become clear in the months that followed. A total of 30 more U.S. high-tech companies (including Adobe and Cisco Systems) were attacked from China. These attacks served to escalate the existing process of changing strategic thinking and caused a paradigm shift in the way the USA approached cyber security. Chinese cyber attacks were now perceived as being so aggressive and all-pervasive that U.S. companies demanded that their government put China under strong political pressure, something they had warned against in the past due to fears of losing access to the booming Chinese market or to larger shareholdings. After spending three months trying in vain to ascertain how much sensitive information had been

29 | Department of Defense, "Strategy for Operating in Cyberspace", Washington D.C., Jul 2011.

spied on or stolen, Google had no choice but to turn to the National Security Agency (NSA) for assistance.[30]

Immediately before this, in the same year, a Canadian university institute identified the GhostNet system. This is an automatic cyber espionage system that infiltrated over 1,300 computers in 103 countries from a server in China. These included numerous computers in government bodies, embassies, international organisations, NGOs and the media. The espionage system searched computers all over the world to steal information and copy e-mails, but it also turned into a gigantic bugging device. Many American companies, including in the IT sector, did not even realise they were being attacked until the GhostNet system was discovered, and until that point they had felt that the NSA was keeping them totally secure. These sophisticated attacks emanating from China had unprecedented potential for destruction. International security experts believe these kinds of attacks are only possible with the support of nation states. And very few organisations outside the defence and intelligence sectors are able to withstand them.[31]

In November 2011 a joint investigation by 14 U.S. intelligence agencies presented the U.S. Congress with their conclusions that China and Russia were the leaders in the state-sponsored digital theft of trade secrets and technology.[32] In 2009 alone, the FBI had proof of over 90,000 cyber attacks on the Pentagon from China. Chinese hackers were also blamed for the temporary shut-down of the House of Commons computer system in Britain.[33] Western

30 | Cf. also John Markoff, "Cyberattack on Google Said to Hit Password System", *The New York Times*, 19 Apr 2010, http://nytimes.com/2010/04/20/technology/20google.html (accessed 23 Jul 2012).

31 | Cf. also Malcolm Moore, "China GloblCyber-Espionage Network GhostNet Penetrates 103 Countries", *Telegraph*, 29 Mar 2009; Kathrin Hille and Joseph Menn, "Hackers in Frontline of China's Cyberwar", *Financial Times*, 13 Jan 2010.

32 | Cf. Thom Shanker, "U.S. Report Accuses China and Russia of Internet Spying", *The New York Times*, 3 Nov 2011; "Chinese cyberspies stealing key data, U.S. analysts say", *CBC news*, 12 Dec 2011, http://cbc.ca/news/technology/story/2011/12/12/china-hackers-us.html (accessed 23 Jul 2012).

33 | Cf. also Duncan Gardham, "'Al-Qaeda, China and Russia, pose cyber war threat to Britain', warns Lord West", *Telegraph*, 25 Jun 2009, http://telegraph.co.uk/news/uknews/law-and-order/5634820/Al-Qaeda-China-and-Russia-pose-cyber-war-threat-to-Britain-warns-Lord-West.html (accessed 23 Jul 2012).

intelligence sources assume there are at least 500,000 hackers who are eager to take part in cyber attacks and spying.[34]

General Keith Alexander, Director of the NSA and Commander of U.S. Cyber Command, speaks at the Center for Strategic and International Studies (CSIS) in 2010. | Source: CSIS (CC BY-NC-SA).

According to a journalist's insider report from 2007, many groups of Chinese hackers work as "freelancers" for the Chinese government, the intelligence services and industry. They have created a tightly-knit network of hackers who are motivated by a mixture of nationalism, technical ambition, financial interest and a personal desire for notoriety.[35] While the Chinese government officially denies all Chinese cyber attacks and claims that its own cyber warfare strategies are wholly defensive, Chinese experts point to the fact that cybercrime is also rocketing in China, and at the same time becoming increasingly professional and well-organised.[36]

34 | Cf. David Barboza, "Hacking for Fun and Profit in China's Underworld", *The New York Times*, 2 Feb 2010, http://nytimes.com/2010/02/02/business/global/02hacker.html (accessed 23 Jul 2012); S. Nandan Andey, "Red Guests. Hacktivism of Chinese Characteristics and the Google Inc. Cyber Atack Episode", *Denkwürdigkeiten*, PMG e.V., No. 63, Apr 2010.

35 | Cf. Scott Henderson, "The Dark Visitor. Inside the World of Chinese Hackers", Oct 2007.

36 | Cf. Kathrin Hille, "Chinese Military Mobilises Cybermilitias", *Financial Times*, 12 Oct 2011, http://www.ft.com/cms/s/0/33dc83e4-c800-11e0-9501-00144feabdc0.html (accessed 23 Jul 2012).

In November 2009, new well-concealed and well-coordinated Chinese cyber attacks against global energy and petrochemical companies were identified. The Night Dragon operations used remote administration tools (RATs) to target and steal sensitive information on ownership and project financing for the purchase of oil and gas fields by Western energy companies.[37] As evidenced by numerous WikiLeaks documents, these kinds of cyber attacks can be traced back to 2002 to semi-independent groups of Chinese hackers such as the Patriotic Hackers or the Honker Union. And it seems that at least some members of the Chinese Politburo have expressly offered their ongoing support for such cyber attacks. However, despite the fact that the USA and the EU have demanded Chinese cooperation in many other areas, they have never called Beijing to account on this for fear of hampering bilateral relations that already have their difficulties.[38] At the same time, the Chinese government is increasingly concerned about cyber attacks on its own computer networks and on the rapidly expanding oil and gas pipelines and electricity networks.[39]

The USA and the EU have never called Beijing to account on Chinese cyber attacks for fear of hampering bilateral relations that already have their difficulties.

In the USA, after the depressing experiences of recent years, industrial espionage is now viewed as the biggest intelligence disaster since the loss of the nuclear secrets in the 1940s. As the *Economist* put it in 2010: "A spy might once have been able to take out a few books' worth of material, now they take the whole library. And if you restock the shelves, they will steal it again."[40] Faced with this, it is unrealistic to think the threat can be eliminated. Over the coming years and decades, protecting operations

37 | Cf. McAfee, "Global Energy Cyberattacks: 'Night Dragon'". White Paper, Santa Clara, 10 Feb 2011.

38 | Cf. Joseph Mann, "US Fears Beijing Still Backs Hacking", *Financial Times*, 5 Dec 2010, http://www.ft.com/cms/s/0/9a0eabc2-0016-11e0-ad1d-00144feab49a.html (accessed 23 Jul 2012); Ellen Nakashima and William Wan, "China's Denials about Cyberattacks Undermined by Video Clip", *Washington Post*, 24 Aug 2011, http://washingtonpost.com/world/national-security/state-media-video-candidly-depicts-chinas-developing-cyber-weaponry/2011/08/22/gIQAqyWkbJ_story.html (accessed 23 Jul 2012).

39 | Cf. Xin Dingding and Wan Zhihong, "China Faces New Risk: Attacks on Pipelines' and Gabe Collins, Smart Moves – China Secures Energy Infrastructure", *Jane's Intelligence Review*, 16 Sep 2010.

40 | Cf. "War in the fifth domain", *The Economist*, 1 Jul 2010, http://economist.com/node/16478792 (accessed 23 Jul 2012).

and production processes to ensure growth and innovation will be a top priority for corporate executives.[41] The present situation where the attacker is clearly superior to the defender is due to the fact that organised crime is better funded in this respect compared to many companies who are unwilling to pay out huge sums for the necessary protection and security. Even recently, countless surveys and expert analyses have shown that: "senior corporate leaders have often too little understanding of the IT security risks and business implications to discuss the trade-offs for investment, risk, and user behavior".[42]

As a result, many companies are still underestimating the security challenges and risks they face, despite the increasing flood of reports in the media. Tellingly, a new analysis by U.S. security firm McAfee in 2011 only differentiates between companies that realise they have been breached and those that have not as yet identified any attacks.[43] Another report published at the end of 2011 that was a kind of annual balance sheet showing the state of worldwide cyber attacks confirmed once again that the threat and capacity for damage of 77 out of 82 selected major espionage attacks had increased and escalated in 2011.[44] In October 2011 a study by the security firm Symantec revealed that there had been 48 coordinated attacks on chemical and defence companies around the world, predominantly in the USA and the UK.[45]

In October 2011 a study by the security firm Symantec revealed that there had been 48 coordinated attacks on chemical and defence companies around the world, particularly in the USA and the UK.

Particularly worrying is a fact that came to light in February 2012. The now-bankrupt American telecommunications equipment manufacturer Nortel had unknowingly been spied on for more than ten years after hackers stole

41 | James Kaplan, Allen Weinberg and Shantu Sharma, "Meeting the Cybersecurity Challenge", *McKinsey Quarterly*, Jun 2011, 1.
42 | Ibid., 3.
43 | Cf. Dmitri Alperovitch, "Revealed: Operation Shady RAT. An Investigation of Targeted Intrusions into 70+ Global Companies, Governments and Non-Profit Organizations during the last 5 Years", McAfee-White Paper, 2011.
44 | Cf. Stewart Baker, Natalia Filipiak and Katrina Timlin, "In the Dark: Crucial Industries Confront Cyberattacks", *Second Annual Critical Infrastructure Report*, McAffee and CSIS, Washington D.C./Santa Clara, 2011.
45 | Cf. Eric Chien and Gavin O'Gorman, "The Nitro Attacks. Stealing Secrets from the Chemical Industry", Symantec-White Paper, Oct 2011.

the passwords of senior company executives. This meant they could read all e-mails, research reports, technical documentation, confidential documents and company financial reports.[46]

STUXNET AND FLAME – HAS THE RUBICON BEEN CROSSED?

The original Stuxnet worm that was discovered in July 2010 infected more than 60,000 computers worldwide. Unlike viruses, worms are able to replicate themselves, and over the last few years they have largely taken the place of viruses.

"What makes Stuxnet particularly earth-shattering is that it was designed to take a never-before-seen leap from the digital world into the physical world. […] Stuxnet has changed the way researchers approach malware and view the security threat landscape."[47] The original Stuxnet worm that was discovered in July 2010 infected more than 60,000 computers worldwide. Unlike viruses, worms are able to replicate themselves, and over the last few years they have largely taken the place of viruses. Stuxnet targeted Iranian uranium enrichment facilities and the Siemens Simatic automation system in Natanz, which was sabotaged in the summer of 2010.[48] The Stuxnet worm was transported to Iran on a USB stick and was only discovered by chance when it unintentionally

46 | Cf. Annika Graf, "Hacker spähten Nortel zehn Jahre lang aus", *Financial Times Deutschland*, 15 Feb 2012, 8; Benedikt Fuerst, "Hacker hatten Zugang zu allem", *Die Welt*, 15 Feb 2012, 12.

47 | So the security software company Symantec, "The Stuxnet Worm", http://www.symantec.com/business/outbreak/id==stuxnet (accessed 18 Oct 2011).

48 | Cf. John Markoff, "Worm Can Deal Double Blow to Nuclear Program", *The New York Times*, 19 Nov 2010, http://nytimes.com/2010/11/20/world/middleeast/20stuxnet.html (accessed 23 Jul 2012); Najmeh Bozorgmehrin, "Web Virus Aimed at Nuclear Work, Says Teheran", *The New York Times*, 27 Sep 2010; John Markoff and David E. Sanger, "In a Computer Worm, a Possible Biblical Clue", *The New York Times*, 29 Sep 2010, http://nytimes.com/2010/09/30/world/middleeast/30worm.html (accessed 23 Jul 2012); William J. Broad, John Markoff and David E.Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*, 15 Jan 2011; David E. Sanger, "Iran Fights Malware Attacking Computers", *The New York Times*, 25 Sep 2010; William J. Borad and David E. Sanger, "Worm was Perfect for Sabotaging Centrifuges", *The New York Times*, 18 Nov 2010, http://nytimes.com/2010/11/19/world/middleeast/19stuxnet.html (accessed 23 Jul 2012); Sandro Gaycken, "Wer war's? Und wozu?", *Die Zeit*, 25 Nov 2011, 31; Alard von Kittlitz, "Stuxnet und der Krieg, der kommt", *Frankfurter Allgemeine Zeitung*, 4 Dec 2010, 33.

landed on the internet. Many cyber experts were shocked by the discovery of this "digital first strike", as until then this kind of highly complex malware aimed at attacking industrial control and monitoring centres had seemed little more than a remote possibility. But now attacks on critical infrastructures and energy control centres have suddenly become much more a reality. President and founder of Kasperky Lab, Eugene Kaspersky, described the Stuxnet work as a "new prototype for future cyber weapons".[49] Other experts fear that this new "precision cyber weapon" will trigger a new arms race.[50] Because of its complexity, the U.S. and Israeli intelligence services were immediately suspected of having developed the "mother of all worms".[51]

Although many experts and the media have described the Stuxnet worm as being the most advanced computer program for infiltrating remote industrial control systems in order to take them over and be able to regulate their power supply and the speed of gas centrifuges in a quasi-autonomous manner, in fact recent studies show that it is less advanced and sophisticated than was originally thought.[52] In Iran it was only able to cause temporary damage to 1,000 of 5,000 centrifuges, so the Stuxnet weapon only had limited success and only served to slow down the progress of Iran's suspected nuclear weapons programme.[53]

However, the Stuxnet worm has changed the perception of the threat posed to industry and the state because it was specifically created to sabotage industrial control systems. The security of SCADA systems (Supervisory Control and Data Acquisition Systems) as the industrial control systems

49 | Cf. "Stuxnet-Wurm befällt iranisches Atomkraftwerk", *Welt-Online*, 26 Sep 2010, http://welt.de/wirtschaft/webwelt/article9884891/Stuxnet-Wurm-befaellt-iranisches-Atomkraftwerk.html (accessed 23 Jul 2012).

50 | Cf. Michael Schrage, "Stuxnet Was about What Happened Next", *Financial Times*, 16 Feb 2011, http://ft.com/cms/s/0/c8142b5a-3a04-11e0-a441-00144feabdc0.html (accessed 23 Jul 2012).

51 | Cf. William J. Broad, "Report Suggests Problems with Iran's Nuclear Effort", *The New York Times*, 23 Nov 2010, http://nytimes.com/2010/11/24/world/middleeast/24nuke.html (accessed 23 Jul 2012); John Markoff, "Worm Can Deal Double Blow to Nuclear Programme and Ari Rusila, Cyber War Has Become a Tool between Political and Military Options", *Europe's World*, 19 Jan 2011.

52 | Cf. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, 02-03/2011, 23-40.

53 | Cf. also Broad, n. 51; Markoff, n. 51.

In August 2011 an expert at a security conference demonstrated how easy it was to for him to break into programmable logic controllers – computers that control automated processes – made by Siemens.

of large, complex and critical infrastructures, like that of information and control centres, is 5 or 10 years behind that of laptops or desktops.[54] In August 2011 an expert at a security conference demonstrated how easy it was to for him to break into programmable logic controllers – computers that control automated processes – made by Siemens even if they were protected by passwords, using a fairly simple, unsophisticated worm.[55]

In October 2011 a Hungarian research institute at the Budapest University of Technology and Economics stumbled upon a new and equally dangerous worm that has been named "Duqu" and classified as a kind of forerunner to future Stuxnet-type attacks. In fact, the researchers were looking for another worm (known as Wiper), but neither they nor other experts were able to find it. The Flame worm was obviously designed by the same team who created the Stuxnet worm as a means of gathering wide-ranging intelligence on industrial facilities, infrastructures and their SCADA systems that could be crucial for launching a later successful attack.[56]

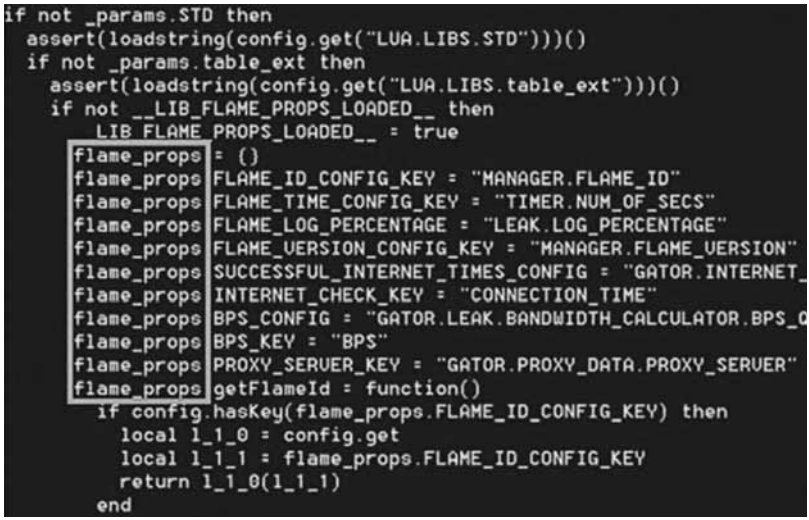
The discovery of the even more complex Flame worm that is 20 times bigger than Stuxnet has once again highlighted the alarming fact that nation states are supporting the development of offensive cyber weapons. Unlike Stuxnet, Flame is primarily a general espionage programme that not only copies data but can also act as a kind of audio-spy by independently activating the microphones on remote computers and smartphones, recording conversations and sending them directly to the originator's servers. This worm

54 | Cf. also Uwe Nerlich and Frank Umbach, "European Energy Infrastructure Protection: Addressing the Cyberwarfare Threat", *Journal of Energy Security*, 27 Oct 2009, 8, http://ensec.org/index.php?option=com_content&view=article&id=219 (accessed 23 Jul 2012).

55 | Cf. Joseph Mann, "US Regulators War Utilities over Cyber Attacks", *Financial Times*, 7 Aug 2011, http://ft.com/intl/cms/s/2/78f94f14-bec0-11e0-a36b-00144feabdc0.html (accessed 23 Jul 2012).

56 | Cf. Symantec, "W32.Duqu. The Precursor to the Next Stuxnet, Version 1.4", 23 Nov 2011; John Markoff, "New Malicious Program by Creators of Stuxnet Is Suspected", *The New York Times*, 18 Oct 2011, http://nytimes.com/2011/10/19/technology/stuxnet-computer-worms-creators-may-be-active-again.html (accessed 23 Jul 2012).

was also used against Iran, but the programming language and software architecture are different, suggesting that it was also developed in the USA. An additional downloadable module also allows Flame to be quickly turned into malware that can cause physical damage to industrial facilities.[57]



```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
      __LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_C
      flame_props.BPS_KEY = "BPS"
      flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props.getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
```

The Flame virus, which was first used in cyber attacks against Iran, has since spread considerably. | Source: AFP (CC BY-NC-SA).

THE GROWING DEPENDENCY AND VULNERABILITY OF ENERGY INFRASTRUCTURES

In the past, energy supplies were decentralised, with each region having its own power plant and a local distribution grid linking producers with their consumers. If the power plant were to break down, then the whole region experienced a power cut. Linking the regional grid to inter-regional transmission grids made the power supply much more secure as it was now possible for regional grids to

57 | Cf. Michael Borgstede, "Ein Virus nach dem Baukastenprinzip", *Die Welt*, 30 May 2012, http://welt.de/die_welt/politik/article106390202 (accessed 24 Jul 2012); Julia Smirnova, "Der Feind am Ende der Leitung hört mit", *Die Welt*, 30 May 2012, http://welt.de/die_welt/politik/article106390001 (accessed 24 Jul 2012); Annika Graf and Joachim Zepelin, "Neuer Computerschädling eifert Stuxnet nach", *Financial Times Deutschland*, 30 May 2012, 7; Annika Graf and Lukas Heiny, "Da ist der Wurm drin", *Financial Times Deutschland*, 7 Jun 2012, 23, http://ftd.de/it-medien/medien-internet/70047098.html (accessed 24 Jul 2012).

transfer power to each other. This also created financial savings, particularly for the producers.

Nowadays these regional networks have spread to cover whole countries and the individual EU member states have been linked together in order to create a single, liberalised energy market for the EU-27 (previously the UCTE, now the ENTSO-E). However, this close coordination aimed at increasing the secure supply of energy for the member states has resulted in a growing dependency on the robustness and stability of each partner's electricity grids. The whole European electricity supply and distribution system is only as strong as its weakest link.[58] If there is any disruption to the frequency and load control processes, which are based on SCADA systems with vulnerable internet connections, or if there are any errors in the coordination between transmission system operators (TSOs) in the respective control regions, then this can quickly affect a great many countries and lead to widespread power cuts. The energy control centres and their SCADA systems are particularly vulnerable in this respect. Should attackers succeed in causing lasting damage to these systems, in manipulating them or even taking them over altogether, this could have a disastrous effect on all other critical infrastructures that depend on a stable electricity supply and secure internet access.[59] Thus, the joint, integrated European energy policies and transnational electricity transmission grids serve to increase energy supply security on the one hand, but on the other they are also open to new risks, particularly in times of crisis.[60]

Should attackers succeed in causing lasting damage to energy control centres this could have a disastrous effect on all critical infrastructures that depend on a stable electricity supply and secure internet access.

58 | Cf. also Alexander Bakst, "The Coming Breakdown of the Power Grid (or Why Electric Cars Can Work only If Consumers Turn to Smart Charging)", *European Energy Review (EER)*, 29 Sep 2011; Karel Beckmann, "The Growing Vulnerability of the European Energy System", *EER*, 14 Mar 2011.

59 | Cf. n. 29.

60 | Cf. Thomas Petermann et al., "Was bei einem Blackout geschieht. Folgen eines lang andauernden und großräumigen Stromausfalls", studies by the Office of Technology Assessment at the German Bundestag, Berlin, 2011, 30 et seq.

Table 4
International power cuts and their consequences

In 2000 the entire EC debit card system collapsed in Switzerland. This was the result of an error in just one computer centre.
In 2003 there were widespread power cuts in 8 U.S. states, as well as in New York City and parts of Canada, causing damages of up to 10 billion U.S. dollars and affecting 50 million people. The power cuts also compromised a wide range of central services and industries. Air traffic and public transport ground to a halt, causing people to be stranded far from home; sewage plants and the water supply stopped working; production was interrupted and emergency communications broke down.
In 2005, a combination of heavy snowfall, ice and gale-force winds led to the Münsterland region of Germany being without power for 5 days, affecting more than 80,000 people in Germany, Belgium and the Netherlands. The losses caused by this power cut were estimated at around 20 million euros.
In 2005, 2007 and 2009, according to the CIA and other U.S. sources, 50 million people in Brazil – one-quarter of the population – were affected by power cuts. In at least one or two cases, this was the direct result of cyber attacks on SCADA systems. However, the Brazilian government has always denied that any cyber attacks occurred.
In 2006 a three-day power cut in Emsland, Germany led to a chain reaction right across Germany and affected 15 million people in 11 neighbouring countries, including Austria, Croatia and Hungary, the effects of which were even felt as far afield as Morocco.

As was made clear in a study by a German Bundestag research institute, large-scale power cuts could result in the ability of every other critical infrastructure to operate effectively being compromised, as they are all dependent on a stable electricity supply. Large-scale power cuts could therefore have an impact on critical food supplies, the security of healthcare systems with their low levels of security, drinking water supplies, sewage disposal, the mobility and transport sectors, not to mention financial services and the maintenance of communications systems, creating either long-term disruption or rendering them inoperable. Within a week there would probably, or at least possibly, be a complete breakdown in public life and public order. A large-scale power cut could destabilise the whole country in a lasting way: "Impact assessments have shown that within a few days it would no longer be possible to guarantee the supply of vital goods and services to the population at large within the affected areas. Public safety would be at risk and the state would not be in a position to fulfil its fundamental legal obligation to protect its people. While the likelihood of there being a long-lasting power cut that affected several federal states at the same time is small,

the consequences if such a thing did happen would be the equivalent of a national catastrophe. The mobilisation of all internal and external powers and resources would not be able to overcome such a catastrophe and could at best mitigate some of its effects."[61]

The effects would not be limited to Germany, as the recent construction of numerous transnational electricity grids and gas and oil pipelines has resulted in an ever-expanding common European energy market, at least as far as physical infrastructure is concerned. On the one hand, this can be a positive benefit for crisis management, such as occurred in 2009 during the last significant gas crisis between Russia and the Ukraine, when certain EU countries with the necessary gas pipeline connections were able to supply each other with energy. On the other hand, the growing integration of national energy markets, especially for electricity, has created a whole series of new dependencies and vulnerabilities that could result in a domino effect across ever-larger geographical regions in the event of a major power cut. However, while the potential consequences of large-scale power cuts have been well researched internationally, the same cannot be said of the effects of an internet blackout.[62]

While the potential consequences of large-scale power cuts have been well researched internationally, the same cannot be said of the effects of an internet blackout.

For this reason, it is a cause for some concern that the cyber risks and vulnerabilities resulting from Germany's shift in energy policy through the introduction of numerous new smart grid and smart home technologies are likely to increase enormously[63], and yet during this restructuring of

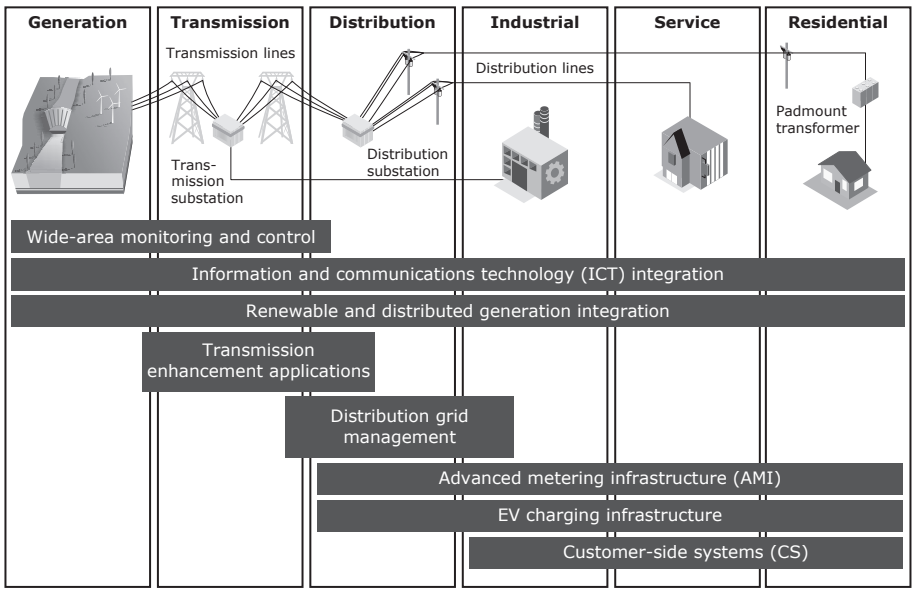
61 | Ibid.

62 | Cf. Ulrich Clauss, "Wird das Internet zusammenbrechen?", *Die Welt*, 7 Mar 2012, 22.

63 | Cf. also *Technology Roadmap. Smart Grids*, International Energy Agency (IEA), Paris, 2011, http://iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf (accessed 27 Aug 2012); Josef Auer, *Smart Grids. Energy Rethink Requires Intelligent Electricity Networks*, Deutsche Bank Research, Frankfurt am Main, 21 Jun 2011; James Osborne, "Smart Grids Move from Research to Early Industzrialisation Phase", *EER*, 9 Feb 2012; Jude Clement, "The Security Vulnerabilities of Smart Grid", *Journal of Energy Security (JES)*, 18 Jun 2009; Guido Bartels, "Combating Smart Grid Vulnerabilities", *JES*, 15 Mar 2011; Ev Tebroke, "Verräterrische digitale Stromzähler", *Welt am Sonntag*, 20 Nov 2011, 65; Claudia Eckert, Christoph Krauß and Peter Schoo, "Sicherheit im Smart Grid. Eckpunkte für ein Energieinformationsgesetz", ▸

the German energy system, these new security challenges have not formed an integral part of domestic political debate. If there have been any discussions about the lack of security standards or about the potential consequences of the introduction of numerous new technologies to increase linkages with the internet, these discussions have taken place between government/ministries, private business and academics in discussion forums that are completely separate from those dealing with the shift in the country's energy policy.

Fig. 2
Smart grid technologies and energy sectors



Source: IEA, n. 63.

Stiftungsreihe 90, Alcatel-Lucent Stiftung für Kommunikationsforschung, Stuttgart, 2011, http://www.stiftungaktuell.de/files/sr90_sicherheit_im_energieinformationsnetz_gesamt_1.pdf (accessed 27 Aug 2012); Harald Orlamünder, "Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein Nachhaltiges Energieinformationsgesetz", *Stiftungsreihe* 85, Alcatel-Lucent Stiftung für Kommunikationsforschung, Stuttgart, 2009, http://www.stiftungaktuell.de/files/sr85_newise_energieinformationsnetz_2.pdf (accessed 27 Aug 2012).

The vulnerability of the electricity sector to even bigger power cuts could well increase in the future as new security concepts and technologies to protect the power grids and to make them more robust are not being developed quickly enough. And yet the introduction of smart grid technologies is the next big step as part of the shift in energy policy, especially in the electricity sector, and is a prerequisite for the combined use of renewable and conventional energy sources, which requires extensive quantitative and qualitative changes to the way electricity is transported both within and between countries. Without these key technologies it will not be possible to achieve either the ambitious goals associated with this shift in energy policy, or German and EU climate policies.

Without smart grid technologies it will not be possible to achieve either the ambitious goals associated with the shift in energy policy, or German and EU climate policies.

A further point that has been largely overlooked in discussions on the implementation of the new energy policy in economic practice is that as a result of the introduction of these new key technologies, the number of linkages between ever larger networks and the regular internet will increase dramatically due to the widespread introduction of wireless networks, cloud computing and the extended use of commodity IT platforms such as smart home and smart grids (intelligent networks), something which could put power supply and management systems at greater risk than ever before. Smart grid technologies use intelligent electricity transmission and distribution systems to provide a constant digital exchange of energy and information. They are based on sophisticated but still cost-effective, metering systems and sensors. The new intelligent electricity meters are expected to cost less than 50 U.S. dollars and will be able to collect and analyse data constantly to help consumers monitor their usage in real time in order to reduce consumption.

However, these intelligent metering systems and networks that serve as distribution and end points for communication and sensor nodes, are in fact automated minicomputers. They include interfaces for wireless networks and link network software, referred to in the industry as "remote disconnect". However, in Europe and the USA, today's generation of smart grid technologies have not been developed with inherent security and defence requirements in mind.

It is only now that these security standards are beginning to be developed and introduced. But if security and defence are not taken into account during the design phase in the development of smart grid technologies, it is unlikely that adequate security solutions will be available once the technologies have already been launched on the market and are being used by consumers.

These advanced digital functions within the electricity infrastructure should improve reliability, efficiency, flexibility and security. However, this means the future electricity grid will become even more dependent on computer-based control systems and therefore more vulnerable to cyber attacks due to multiple contact points with the internet. Any increase in the number of these internet contact points will dramatically increase the system's vulnerability, but without the kind of overall system robustness that existed in the past.

CONCLUSIONS AND OUTLOOK

The identification of the Stuxnet computer worm in June 2010 demonstrated the vulnerability of SCADA systems at energy and other industrial control centres. Not only other countries, but also terrorist groups and international organised crime, can copy, modify and enhance complex malware, such as Stuxnet, Flame or Duqu, for counterattacks on creators. In view of the advances being made in computer technology and dramatic increases in vulnerability, many security experts believe it is only a matter of time before this becomes reality. Cyber weapons are invisible, anonymous and can have devastating effects. When they are used, the boundaries between offensive and defensive, private and state-run all vanish. But above all, at present it remains impossible to identify attackers. It is precisely for this reason that a steady, sharp increase in cybercrime should be feared as much as an accelerating cyber weapons arms race.

When cyber weapons are used, the boundaries between offensive and defensive, private and state-run all vanish. But above all, at present it remains impossible to identify attackers.

The widespread introduction of different kinds of smart meters and other intelligent home technologies, along with smart grid systems, and the connection to the internet of systems that used to operate autonomously mean that all

areas of life are rapidly becoming more and more interdependent – and in the process inevitably allow for many new possibilities for attacks. It is vital that security and data protection are afforded much greater priority in future. At the same time, critical infrastructures must be made more robust if it seems impossible or undesirable to disconnect them from the regular internet and build a parallel intranet. Thus, in future, redundancies and reserve capacities will more than ever take on central strategic significance for energy supply security, particularly for electricity and network stability, in order to be armed to deal with entirely new cyber threats and the risks of large-scale power cuts.

Both public and private sectors must develop comprehensive, multi-layered security strategies that are integrated with business development and form part of an appropriate EU-side security concept.

However, the German government's long-term energy strategy is to reduce such redundancies and reserve capacities that maintain energy supply security and instead to make Germany a net importer, even of electricity to supply critical infrastructures. This harbours some major risks in terms of securing against future cyber attack capabilities on industrial control and monitoring centres. Any kind of disruption to the electricity sector can affect other locations, industries and sectors across the whole of the EU. Both public and private sectors must develop comprehensive, multi-layered security strategies that are integrated with business development and form part of an appropriate EU-side security concept.

The more the EU integrates national energy and electricity markets, the more they increase energy supply security and reduce costs. But on the other side of the coin the increasing interconnectedness of the national markets also increases the likelihood of a domino effect. In future, the security and resilience of national critical energy infrastructures can no longer be ensured and enhanced by purely national, uncoordinated strategies. Critical energy infrastructure protection (CEIP) must be expanded and intensified by the EU, NATO, the Organisation for Security and Cooperation in Europe (OSCE), the G8 and other international bodies.

The operators also have limited financial and human resources to dedicate to protecting their infrastructure systems. It is therefore important to use all available resources as efficiently and effectively as possible by weighing up

eventualities and setting corresponding priorities to ensure appropriate risk management. In most cases, companies can equip themselves to fight cybercrime with a fairly modest outlay. 90 per cent of all current data leaks could be prevented by regularly updating their software programs. Telecommunications companies such as Deutsche Telekom have begun setting up "honeypot systems" to attract hackers to websites where they will find little of value. In this way they can study the hackers, their latest techniques and attack methods and identify security lapses in their own systems that may be used by cyber criminals to access IT and communications networks.

Of course it is impossible to fully protect public utilities and critical infrastructures from physical or cyber attacks. But it is vital to minimise the risks without having an overly negative impact on productivity and normal operations. Any professional evaluation of security and risk has to include both physical and cyber security, along with SCADA and distributed control systems (DCS), communications security, network security, transmission security, production security and biological/chemical issues.

However, the main security challenge facing companies and national strategies for the protection of critical infrastructures that are largely privately-owned is the need for a fundamental shift in corporate cultures. The first step is to break down the venerable tradition of "keeping quiet". Successful attacks have increasingly led to companies being blackmailed and paying hush money to cyber criminals in order to protect their reputation in the market. Almost half of all companies surveyed by the German technology association Bitkom admitted they had no disaster recovery plan in the event of an attack. One in four companies even confessed they would rather not report it to the police if they were the victims of an attack or if they identified a data leak.[64]

One in four companies confessed that they would rather not report it to the police if they were the victims of an attack or if they identified a data leak.

The situation in Germany is made even more difficult by the fact that at present companies are only obliged to report attacks in exceptional cases. It remains to be seen what

64 | Cf. Florian Eder, "EU verschärft Kampf gegen Hacker", *Die Welt*, 27 Mar 2012, 11.

benefits arise from setting up a compulsory registration office, as is the case in some countries, or from the attempt by the "Allianz für Cybersicherheit" (Cyber Security Alliance) to set up a central, voluntary system for reporting cyber attacks in order to encourage the anonymous exchange of information and knowledge. On the other hand, the European Commission has declared that in future companies will have to take data protection more seriously and they will have a duty to disclose the extent of any cyber attacks. More than ever before, the private and public sector will have to "think the unthinkable" when analysing future cyber security challenges, and if necessary they will have to be prepared to abandon well-trodden avenues, strategies and organisational structures.