EUCERS ENERGY TALKS 2

By Shiraz Maher

KING'S College LONDON

EUCERS European Centre for Energy and Resource Security

acatech DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Konrad Adenauer Stiftung

CONTENTS

I. Preface

In 2013, the European Centre for Energy and Resource Security (EUCERS) together with the German National Academy of Science and Engineering (ACATECH) and the Konrad Adenauer Foundation (KAS) in London hosted a series of round-table discussions at King's College London. After the successful cooperation and organisation of energy talks in 2012 by EUCERS and KAS, the second series - now with partner ACATECH - was to promote innovative and creative thinking around the issue of energy resilience. This led to the arranging of five probing round-tables on the topic.

The philosophy behind this series was to help participants understand the challenges surrounding energy resilience within an international context in two distinct ways. The first concerned the idea of energy independence or, at least, diversification. The topic was particularly timely given how much emphasis was placed on the issue during the 2012 US Presidential election by both candidates, and because of recent unrest across parts of North Africa and the Levant. The second issue concerned the growing threat from terrorism, cyber-attacks including both espionage and sabotage. It was felt this was particularly relevant given the ever-increasing interconnectedness of regional and national energy grids in the European Union.

The series was hosted at King's College London and consisted of five separate panel discussions on distinct aspects of energy resilience and vulnerability: "Europe's Vulnerability to Energy Crises" (12.3.2013), "Building Resilient Energy Infrastructure Beyond Europe's Borders" (8.4.2013), "The Danger of Blackouts – Electricity Security as the Achilles Heel of Resilient Energy Infrastructure?" (3.5.2013), "Challenges and Prospects for an Integrated Energy Infrastructure in Europe" (18.6.2013) and "Terror Attacks on Energy Infrastructure – A Growing Threat?". It attracted participation from members of the public, politicians, academics, students, the media and energy sector professionals. These talks operated in a 'round-table' format with a moderator chairing the discussion between two or more speakers and an invited discussant. The majority of time was allocated to inviting questions and comments from the audience, underscoring the purpose of the series – which was to engage, inform, and promote innovating thinking among our participants. Each session attracted between 30-50 participants.

This report begins with an article from Professor Dr Friedbert Pflüger, Director of EUCERS, on resilient energy systems, before presenting a summary of the round-table workshop series.

II. Energy Security Turns 100!

Thoughts on resilient energy systems

By Friedbert Pflüger

On July 17, 1913, almost exactly 100 years ago, the First Lord of the Admiralty, Winston Churchill, took the floor of the British House of Commons. British warships, he proclaimed, would no longer be powered by coal, but by oil instead in order to become faster and more cost-efficient than the German fleet. This, however, also meant that the Royal Navy had to substitute domestic coal with Persian oil. Countering the critics in the opposition, he insisted that London should never become dependent on a single country, route, energy source or (oil) field: "Safety and certainty in oil lie in variety, and variety alone." – Churchill had thereby outlined the central theme for all future debates on energy security: the diversification of energy supplies.

Sixty years later, in October 1973, OPEC's oil embargo shocked the West. Neglecting Churchill's warning, the industrialized world had, for some time already, fallen into dependence on oil-producing countries, particularly from the Middle East. Now oil prices quadrupled, the economy slowed down and overnight it became clear that the world's power balance had shifted: the producers in the global "South" had become a political power. For the first time, the "North" appeared vulnerable to the "oil weapon".

In the wake of the Oil Crisis, energy security became the core concern for the industrialized Western nations. At the 1974 Washington Energy Conference, they agreed on a concerted reaction in the event of future disruptions of energy supplies. This is how, among other things, the so-called strategic oil reserves came about, as well as the International Energy Agency (IEA), which was set up as an institutional counterweight to the OPEC-empire (Daniel Yergin). The IEA, based in Paris, lived up to its founders' expectations. Its analyses and forecasts of developments in energy policy today form a common base for science, business and politics alike. It also put forth the now widely accepted definition of energy security as "an uninterrupted availability of energy sources at an affordable price."

The importance of energy has only continued to increase in a globalized and digitalized world. Today, hardly anything is conceivable anymore without energy, be it drinking water, television, computers, or phones. In the absence of the global network of transportation, cooling systems and stores, our supply chains providing people with food and essential goods would fail. Therefore, the uninterrupted supply of energy has become all the more important. Energy security is a matter of life or death for every modern society. The advent of renewable forms of energy in the last decade – they can at least cover about two percent of the global energy demand (excluding hydro-power) – has barely done anything to diminish the dominance of fossil fuels. Even by 2035, around eighty percent of the energy demand will be satisfied by oil, natural gas and coal (in almost equal shares, by the way) (IEA World Energy Outlook 2012).

Friedbert Pflüger and Anita Orban at 4th EUCERS/ACATECH/KAS Energy Talk

Energy security in the international context will therefore continue to depend on uninterrupted supplies of fossil fuels for the foreseeable future.

Supply security at an affordable price is an extremely complex and fragile matter, and hence continuously at risk. In this context, we can distinguish seven central risk factors:

SEVEN RISK FACTORS FOR ENERGY SECURITY

1. Wars, crises and conflict in energy-producing countries can lead to disruptions of production and supply of energy that affect the global economy. The Iranian Revolution of 1979, the First Gulf War of 1990/91 or the complete halt of the Libyan oil production as a consequence of the war of liberation of 2011, for example, all had drastic effects on supply chains, energy prices and, as a consequence, the economic situation in importing countries. Similarly, the general strike in Hugo Chavez' Venezuela of 2002 or the Iraq War of 2003 had serious effects and contributed – alongside other factors that will be discussed later – to a continued surge of the oil price, which eventually hit $140 per barrel, exacerbating the global economic crisis.

2. Political extortion as a consequence of a one-sided dependence on an energy producer is another risk factor for an uninterrupted supply of energy at an affordable price. The dominance of Russian gas supplies to parts of Europe, in particular the Central and Eastern European countries, meant that gas prices were no longer determined via supply and demand mechanisms, but decided politically, depending on good conduct by the respective government. The disruptions of Russian gas supplies to the Ukraine of 2005/06 and 2009 caused a supply crisis in several Central European countries, even though its actual effect was outmatched by the fears of a massive demonstration of power by Russia. The two gas crises, which Moscow should not be blamed for one-sidedly, sparked an intensification of European discussions over energy security and gave new impetus to plans for more diversification of the gas sector through alternative supplies from the Caspian region via the "Southern Corridor". In addition to that, they led to the inception of a genuine European energy policy and the appointment of a proper EU-Commissioner for energy (Günther Oettinger).

3. An impending re-nationalization – and even energy imperialism – today are real threats for a global supply system based primarily on the interplay of supply and demand. More than eighty percent of conventional reserves of oil and natural gas are produced by state- or semi-state-owned energy companies, i.e., they are directly or indirectly dependent on the political leaders of that respective country, who are well aware of the political relevance of the resources they control. Increasing scarcity of natural resources against the backdrop of a dramatic growth of the world's population and its thirst for energy – global demand will increase by one third by 2035 –will make it all the more tempting to use one's riches for nationalist, or even imperialist, ends. China's determination in securing access to sources of energy and raw materials across the entire globe ranks among the most significant phenomena of the early twenty-first century.

4. Terrorist attacks against energy infrastructure, i.e., on the routes of oil and LNG tankers as well as on pipelines and oil rigs, can also pose a threat to supply security at an affordable cost. In 2006, terrorists in the Niger-Delta (in Nigeria) caused a dramatic reduction in oil production. The Arish-Ashkelon pipeline between Egypt and Israel was attacked 13 times in the year following the fall of Mubarak, with dramatic consequences for Israel's energy security. Forty percent of Israel's supplies depend on Egypt; for neighbouring Jordan that figure is eighty percent. As recent as January 2013, Islamist terrorists attacked BP's oil production in the Algerian desert and kidnapped employees of that company. Anywhere around straits – from the Strait of Malacca to the Strait of Hormuz and the Bab-el-Mandeb between Yemen and Somalia – terrorists and pirates lurk, often in collaboration.

5. Cyber terrorism against critical energy infrastructure represents a growing and often underestimated danger to energy security. Frank Umbach recently pointed out that, although the US-military is forced to make cuts in their budget, the Pentagon's Cyber Command was increased from 900 to 4 900 personnel. President Barack Obama recently warned that enemies of the United States could attempt to sabotage its energy infrastructure, particularly its power grids. The head of the US national intelligence service, James Clapper, added that such attacks constituted "the most immediate threat." What if a cyber attack succeeded in disabling the cooling systems of nuclear power plants? In 2012, Austrian author Marc Elsberg wrote a political thriller on the dangers of cyber terrorism for Europe's electricity supply that he recently presented at the Forum FAZ/ Munich Security Conference.

6. Natural disasters are a real threat to supply security, as the two storms Katrina and Rita demonstrated in 2005. These storms destroyed about 170 offshore oil platforms in the Gulf of Mexico. Almost a third of the American oil production and its refining capacity was lost – with far-reaching and long-lasting consequences for supplies across the entire country. Even worse were the consequences of the earthquake and the ensuing tsunami on March 11, 2011 in Japan: they led to the death of thousands of people and a "beyond design-basis accident" at the Fukushima Daiichi nuclear power plant, with dramatic consequences for Japan's society and economy. Beyond disasters of such magnitude, reinsurance companies report that the number of devastating floods and storms is on the rise – not least as a consequence of climate change. And natural disasters like these are usually accompanied by short- or long-term disruptions of energy supplies. These threats will increase along with the progression of climate change: monster storm Sandy of October 2012, which took six lives in New York alone, forced the evacuation of 375 000 people, and left 8 million people without electricity for several days, was only a foretaste. Only a few years ago, it was

5th EUCERS/ACATECH/KAS Energy Talk

inconceivable that storms of this magnitude would appear as far north. Climate change also brings new dangers to other parts of the world, both, for people and energy supplies: What, for example, will it mean for Russia when the permafrost regions of Siberia get perpetually warmer? What consequences will there be for supplies to Chinese cities when Himalayan glaciers continue to melt and the big hydro-power plants do not pro- duce enough electricity any longer?

7. Technical failure, often related to human error, is and continues to be a threat to energy security. Technology will never be perfect; a residual risk always remains. The tragic disaster of Chernobyl in 1986 is a prime example, but even comparatively lesser accidents like the Exxon Valdez oil spill of 1989 in Alaska can, besides damage to humans and ecosystems, also affect regional energy supplies. Greater threats for energy security result, for example, out of the hitherto unresolved final storage question of nuclear fuel elements, but also the theoretical possibility that chemicals used in "fracking" – the technology involved in the production of fossil energy in shale formations – come in contact with groundwater. Even just the hypothetical scenario of accidents like these, caused by the interaction of humans and technology, can lead to a reduction in public acceptance of such forms of energy production.

So how should we deal with these threats? The key is to build resilient energy supply systems. In 2012, the National Academy of Science and Engineering (ACATECH), in close collaboration with the Federal Government of Germany, formed the working group "Resilien-Tech." Headed by the Director of the EMI at Freiburg (Fraunhofer Institute), Professor Dr Klaus Thoma, the working group focuses on the integration of security aspects – "resilience by design" – with an eye on the state, society and the economy. This includes the issue of resilient energy supplies.

SEVEN MEASURES TO BUILD RESILIENT ENERGY SYSTEMS

A resilient energy system is defined by its ability to withstand interruptions or to prevent failure through protective measures, respectively. Churchill's century-old demand for variety, i.e., diversification, takes centre stage in this endeavour.

1. DIVERSIFICATION AND ENERGY INDEPENDENCE

Churchill had defined the most important task over 100 years ago: diversification. Only a variety of energy sources, producing countries and supply routes can bring security. The effort to overcome dependence in the wake of the OPEC oil embargo led to Richard Nixon's "Project Independence" of November 1974, in which he demanded American energy independence from foreign countries. This goal, confirmed by practically all US presidents since Nixon, might finally be realized half a century later: by the mid-20s of this century, the United States might become independent of oil and gas imports as a result of the shale revolution!

2. DECENTRALIZATION

Another possibility to protect complex energy systems, especially to help prevent major disruptions or to limit their effects, respectively, lies in the introduction of complementary, decentralized supply systems. Renewable forms of energy in particular are well suited for this purpose: wind, PV, solar thermal, biomass, geothermal and, last but not least, hydro-power. Many households, but also small and medium-sized businesses are now trying to become largely independent of the main grid through such decentralized energy sources. As renewable forms of energy are subject to high output fluctuations, they currently still rely on conventional energy sources for "back-up" – at least as long as storage technologies remain inadequate.

3. HIGHEST SECURITY, EFFICIENCY AND ENVIRONMENTAL STANDARDS

Security and environmental standards may be expensive. But in the end, they serve everybody because of their pre-eminent importance for public acceptance of the respective energy source. While the hurricanes Rita and Katrina cost the lives of many and caused widespread destruction, particularly in the city of New Orleans, it is due to highest-level standards that no oil was spilled into the Gulf of Mexico despite many drilling rigs being destroyed. BP, on the other hand, incurred high financial and image costs in 2010 as a result of insufficient security and environmental standards in the context of the sinking of its Deep- water Horizon offshore drilling rig. The auto and petroleum industry, in turn, owe their continued acceptance in Europe to the dramatic progress they achieved in efficiency and environmental standards.

4. DIALOGUE BETWEEN PRODUCERS AND CONSUMERS OF ENERGY

Maintaining an intensive and trustful dialogue between importers and exporters of energy is of central importance when it comes to the prevention of disruptions in the global energy system. It is particularly relevant to understand the interests of the other side, because the meaning of energy security is very different for producing countries than for consumers: to the former, energy security does not mean supply security, but "security of demand". The big petroleum exporters, such as Russia, Saudi Arabia, Libya, Angola or Venezuela, depend on regular sales of their resources at an acceptable price from their point of view. Just as higher oil or gas prices affect the economies in Western countries,

lower energy prices reduce those states' income, which can easily affect political stability at home. The IEA plays a particularly important role in this regard, but all bilateral and multilateral encounters – from state visits to academic conferences – contribute to maintaining a dialogue and fostering mutual understanding. Likewise, the work of political foundations and chambers of commerce, and especially the cooperation between managers, engineers and workers in joint projects, help build mutual understanding of interests and cultural differences, and create transparency through the comparison of data and analyses– which in turn helps build trust. A particularly important task in this regard today is the integration of China and India into the various forums of the international energy dialogue.

5. INTEGRATING THE YOUTH: JOBS

The rapid population growth in many exporting nations, especially in the Middle East, Africa, and Latin America, means that, even if their economies grow, these countries cannot create nearly enough jobs for their younger generations. Around half the population in Algeria, Libya and Saudi Arabia, and over sixty percent of Iraqis, are under the age of 25. The production of oil and gas is capital-,but not labour-intensive, i.e., those industries create few jobs directly. Unemployment and poverty experienced by millions of young people provide fertile ground for political radicalization on which Islamist extremists can sow the seeds of their violent ideas. Therefore, it is in Western countries own interest to do everything they can to help petroleum states diversify their economies and provide job-training opportunities for their youth. The work of development agencies, from the GIZ to the political foundations, is particularly relevant when it comes to improving the prospects of many young people.

6. PREVENTIVE MEASURES BY POLICE AND MILITARY

It was US President Jimmy Carter who formulated the 1979-doctrine according to which any attempt of foreign forces at gaining control over the Persian Gulf would be regarded as "an assault on the vital interests of the United States of America" that would be countered by any means necessary, including military action. Ever since, the United States has continuously considered it a top priority to secure the energy lifelines, i.e., the uninterrupted flow of Middle Eastern oil and gas. To be fair, there may be good reasons to be critical of specific political and military measures undertaken by Washington in this context. Nonetheless, it is a fact that Europeans have benefited in equal measure from the United States' commitment to securing the energy routes. Free movement by tankers through straits, protection from pirates and terrorists, the collection of intelligence on terrorist groups and the fight against them domestically – all these tasks call for continued protective action by police and military forces. The Europeans will likely have to increase their contribution in this domain, given that the United States' readiness to act militarily overseas will probably decline as a result of the "shale revolution" in North America.

7. DISASTER CONTROL

Finally, resilient energy supply systems need adequate and readily deployable emergency measures in the event of a catastrophic supply crisis in the wake of a terrorist or cyber attack, as well as in case of an accident or natural disaster. In countless calamities ranging from Chernobyl and Fukushima to storms such as Katrina or Sandy, but also Deepwater Horizon, we had to learn that few emergency plans and guidelines were in place, e.g., for evacuations, medical care, emergency shelters, etc.; in particular, there were no clear rules allocating responsibilities. But re-establishing supply security quickly crucially depends on swift action in case of an emergency.

III. EUCERS Energy Talks organised in conjunction with ACATECH and KAS

The EUCERS round-table series on energy resilience began in Spring 2013. The format involved between two or three keynote speakers giving a set of opening remarks, followed by a rigorous discussion including participants. A light lunch was provided after each session, allowing attendees an opportunity to both continue their discussions and to network, in a more informal capacity.

1st EUCERS/ACATECH/KAS Energy Talk

FIRST EUCERS/ACATECH/KAS ENERGY TALK: EUROPE'S VULNERABILITY TO ENERGY CRISES

The first session took place in March 2013 and it was to provide a general assessment and overview of the issues surrounding energy resilience and its significance. This was done in order to set the tone for the subsequent roundtables by establishing the importance of the series and explaining the key issues around energy resilience. It also offered newcomers an opportunity to gain a basic understanding of the subject matter, on which they could then build their knowledge in subsequent workshops.

This session was addressed by presentations from Dr Thomas Rid, Reader at the Department of War Studies, King's College London and a non-resident fellow at the School for Advanced International Studies, Johns Hopkins University, in Washington, DC. and Dr Frank Umbach, Associate Director, EUCERS. Another invited speaker, Jörg Asma, Partner at KPMG and member of the Resilient Tech Working Group, ACATECH – National Academy of Science and Engineering in Germany – was unfortunately unable to attend due to adverse weather conditions.

Professor Dr Friedbert Pflüger, Director EUCERS and Claudia Crawford, Director London Office of the KAS opened the meeting by noting the timely relevance of considering matters related to energy security and vulnerabilities. Pflüger remarked that the issue of energy resilience was a consistent theme addressed by both of the leading American Presidential candidates in 2012. This was coupled with an upswing in reports about Chinese hacking efforts against the United States and its interests.

Dr Frank Umbach spoke about on-going international vulnerabilities, which have the potential to affect multiple countries. The terrorist attack on the In Amenas gas installation in Algeria was one event, which underscored this point. Umbach also explained the vulnerabilities of the electricity grid where mitigation of disruption risks proves significantly harder than it can when planning contingency measures for disruptions to oil and gas. This is mainly due to a lack of understanding and because of associated coast considerations. Given that all critical infrastructures rely – in one form or another – on electricity, this makes its security a vital matter.

Dr Thomas Rid focused on cyber-attacks by exploring seven of the most prominent cases in the field. In general, Rid's research has revealed that most of these cases were not really attacks at all, but were instead

Panel at 1st Energy Talk

the result of misfortune, coincidence, poor maintenance, or human error. Indeed, with regards to sabotage, the only real notable example relates to Stuxnet, which was produced by joint US-Israeli efforts. Even that case, perhaps the most dramatic incident of a cyber-attack, should be put in context Rid argued. Stuxnet only had one target – Iranian computers linked to its nuclear programme. As a piece of malicious programming it is redundant and useless against every other target. Stuxnet also took about seven years to produce, which underscores how difficult it can be to launch effective cyber-attacks. Finally, Rid noted that cyber-attacks are more likely used in cases of espionage rather than sabotage. The latter is not designed to influence or affect the host it infects adversely. Instead, its primary aim is to steal knowledge and information, but it is not aimed at disruption and would not therefore be likely to pose a big threat to energy security.

SECOND EUCERS/ACATECH/KAS ENERGY TALK: BUILDING RESILIENT ENERGY INFRASTRUCTURE IN EUROPE AND BEYOND

The second EUCERS/ACATECH/KAS talk took place in April and explored what coordinated European action can do to promote resilient infrastructures across the continent and beyond. This allowed participants to explore what best practices might be developed going forward in order to counter challenges and risks.

Opening remarks were made by Professor Dr Klaus Thoma, Head of the Fraunhofer Institute for High Speed Dynamics, Ernst-Mach-Institute in Germany and a member of ACATECH; and Dr Yolanda Garcia-Mezquita, from the European Commission's Directorate General for Energy. The round-table was chaired by Hans-Hartwig Blomeier, new Head of the KAS Office in Great Britain and Shiraz Maher, KAS Fellow 2012/13 at EUCERS.

Professor Dr Klaus Thoma started the meeting by explaining the specific challenges for building resilient infrastructures such as increased urbanisation and the threat from terrorism. He also noted the difference of working across different infrastructures where change and innovation operates on very different timescales. For example, ICT and automobile innovation tends to occur almost yearly while the sewage infrastructure or urban structure changes over centuries. Creating intra-structure resilience can therefore be extremely difficult to achieve. To illustrate this, he highlighted the Desertec Foundation's proposed plans to implement a clean power programme. With a large part of it based in North Africa, the problems of political instability and terrorism are dramatically captured. Furthermore, the issue of technological innovation is also relevant here relating to solar power, photovoltaics, and high voltage direct current transmission.

Dr Yolanda Garcia-Mezquita contrasted the theoretical and engineering based approach of Prof Dr Thoma by highlighting practical measures being taken by the European Commission to address some of these challenges. She noted how the Commission is trying to find new ways to incentivise drivers for investment so the private sector can be encouraged to address some of these problems. This has been done, to an extent, she noted with integrating and interconnecting markets across Europe. Indeed, she pointed out that the Commission does not just want to empower private companies – but also individual consumers through initiatives like smart meters. Yet, Dr Garcia-Mezquita also explained how European interdependency

From left: Yolanda Garcia-Mezquita, Hans-Hartwig Blomeier and Klaus Thoma

Klaus Thoma and Shiraz Maher

can also present problems such as during the Russian-Ukrainian gas dispute in 2009 which had ramifications across the continent as a whole.

During the round-table participants quizzed the speakers and debated the issues they had raised. Participants spoke particularly robustly on topics relating to whether the open market can really accommodate future energy needs. Many argued that the ratio of return on investment to risk and time made it unattractive for potential investors. There was a broad consensus that this problem would be insurmountable without government intervention to guarantee minimum unit prices and protections. Indeed, many felt this related not just to infrastructure but also to the development of new technologies. To complement purely pecuniary measures, it was also suggested that legislation could play a role, although, again, it was felt this would only work if supported by financial assurances from government.

THIRD EUCERS/ACATECH/KAS ENERGY TALK: THE DANGER OF BLACKOUTS: ELECTRICITY AS THE ACHILLES HEEL OF ENERGY INFRASTRUCTURE

The Third EUCERS/ACATECH/KAS talk took place in May. It is often said that securing electricity security is particularly difficult because of associated costs and a lack of understanding about the issues involved with it. This makes the grid particularly susceptible to blackouts, representing an Achilles heel in the energy resilience infrastructure. This round-table explored both the exposure or vulnerability of the grid to current threats, and what steps might be taken to mitigate those risks.

Presentations were made by Jörg Asma, Partner with KPMG in the department of IT Advisory with responsibility for information protection business resilience in Germany and the EMA. He was joined by Dr Sarah Mander, deputy-leader of the energy programme at the Tyndall Centre, Manchester University, who focuses heavily on climate change mitigation and social responses to energy crises.

The session was chaired by Professor Dr Friedbert Pflüger, Director of EUCERS and Hans-Hartwig Blomeier, Head of KAS office in Great Britain. Pflüger opened the session by noting the numerous challenges concerning energy infrastructure, not least its ageing and insufficient nature. Furthermore he highlighted the additional strains posed by new energy sources such as wind and solar, which create instability in energy grids, and the ever increasing threat of cyber attacks.

Jörg Asma opened his statement by focusing on the threat from cyber attacks. He pointed out that there are two very different types of cyber attacker. The first are criminals who often seek financial gain from their activity. The second, however, are an altogether (but increasing) community of activist-hackers ('hacktivists') who typically have no monetary interest in launching an attack. Instead, they are motivated by ethical or moral interests and this community now represents the

Advanced Persistent Threats and Energy Supply

BY JÖRG ASMA

Cybersecurity is one of the key topics that is being discussed nowadays however not only by security specialists, but also by the c-level members. Cybersecurity has become a boardroom issue.

In 2006 the United States Air Force (USAF) created the acronym APT which means advanced persistent threat. Yet what is so advanced about these threats? Hackers using APT techniques have insight knowledge about the administration of IT systems' infrastructures and other important components. Each and every individual using IT systems leaves a footprint in the systems. As do these kinds of attackers. Their footprint looks very much like IT administrators, who are regularly using the system. Their tools are not unspecific unlike those of commodity hackers or hacktivists. Their intention is to exfiltrate data from networks and systems without being recognized. Their activities usually start with an information gathering phase about the target and its environment such as colleagues, private contacts, family etc. to establish the best way in. Tools being used are very specific and tailor-made to hit the persons or systems that have been identified during the information gathering phase. Usually, hackers using APT techniques start to scan for detection measures before deploying the tools to break in. When deployment has been successful new credentials for other systems and targets are collected, for example of the real target, which is usually not directly in focus when the attempt to break in starts. Typical symptoms for an ongoing APT are the existence of well configured viruses and malicious codes, which are usually not detected by antivirus systems, as well as spear fishing attacks on users.

Hackers will then start exfiltrating data while trying to hide the existence of malicious configurations and codes. This is a very sensitive step since this means that not large amounts of data may be transmitted, but only relevant data with their extraction destination continuously varying.

greatest threat in the hacking space. Asma also pointed out the difficulty of detecting hacking operations, which can usually operate for 4-6 weeks before any detection has occurred. To highlight this, Asma offered a case study where KPMG was asked by a client to detect the vulnerability of its software controlling wind farms. He noted the relative lack of sophistication of the security software protecting that infrastructure, and explained how it was hacked. Furthermore, he explained how employees are becoming increasingly susceptible to malicious code emails through their use of social media such as Facebook and LinkedIn, which can reveal their interests.

Dr Mander spoke of the need to mitigate threats by moving to a de-carbonised electricity grid by 2030, and reducing carbon emissions by 80% by 2050. She also noted how electricity networks need to do more in order to adapt to the current pressures being applied to them. This includes boosting operational resilience by updating ageing cables and overhead lines. Moreover, Dr Mander pointed to extreme events such as weather disruption, which can also cause disruption to electricity supply. She noted that it is not just electricity providers who need to explore ways of developing infrastructure resilience to such events, but that better public awareness is also needed to help educated the public to cope with these events when they occur. In essence, she noted a five-point plan for building resilience around the ideas of: resistance, reliability, redundancy, response, and recovery.

A vibrant discussion followed with participants questioning the speakers and debating the issues. Participants spoke about the increasing public disdain for above-the-ground electrical cables and the pressure to have more of them underground. This also led to a discussion of planning regulations regarding the building of new pylons. Dr Frank Umbach also spoke about cyber attacks noting that cyber crime can cost $40 billion annually, and that such attacks are increasing by 30% per annum. He noted that, in this context, the advent of smart home technologies would create new vulnerabilities and costs. This was an aspect, Dr Umbach argued, that manufacturers are overlooking. In 2009, for example, it was noted that both Russia and China attacked the U.S. electricity grid with viruses. Overall, the U.S. reports that attacks on its critical infrastructure increased by 52% from 2011 to 2012. Germany also faced similar attacks.

FOURTH EUCERS/ACATECH/KAS: CHALLENGES AND PROSPECTS FOR AN INTEGRATED ENERGY INFRASTRUCTURE IN EUROPE

The fourth EUCERS/ACATECH/KAS event took place in June and examined what has gone right – and what has gone wrong – with integrated energy plans in Europe. It also asked, what greater cooperation across Europe might look like in the future while also exploring challenges to greater cooperation.

Presentations were made by Dr Anita Orban, Hungary's Ambassador-at-Large for Energy Security, Thomas Dimitroff, Partner at the Infrastructure Development Partnership LLP and Tora Leifland Holmström, who is a Government Affairs Advisor for the Trans Adriatic Pipeline (TAP).

Speakers and participants were welcomed by Professor Dr Friedbert Pflüger, Director of EUCERS and Hans-Hartwig Blomeier, Head of KAS Office Great Britain. Pflüger, who also chaired the session, noted the political importance placed on energy infrastructure within the European Union. Furthermore, he gave an example of one aspect of what an integrated system might look like with

4th EUCERS/ACATECH/KAS Energy Talk

Panel at 4th EUCERS/ACATECH/KAS Energy Talk

From left: Friedbert Pflüger, Anita Orban, Tora Leifland Holmström and Hans-Hartwig Blomeier

reference to the interconnector pipeline, providing bi-directional transport capabilities.

Dr Anita Orban focused on the energy concerns of Central European states, noting that the issue had taken on renewed importance after the 2006 energy crisis resulting from the Russia-Ukraine gas dispute. This political importance is given further significance, she noted, given that the EU Presidency is revolving back to Central European powers. Dr Orban also acknowledged that the shale gas revolution is also having an indirect effect on Central European energy policy with Poland – which has Europe's largest reserves – now trying to harness the potential of its shale deposits. Finally, Dr Orban noted that Central European countries have three primary energy goals. The first is to achieve energy security. The second is to speed up energy market integration. The third is to secure stable and competitively priced energy.

Thomas Dimitroff opened his presentation by urging attendees to consider the question of integrated infrastructures from the perspective of producer/exporter countries. To highlight the priorities from this perspective, Dimitroff spoke about the then ongoing tender between Nabucco and TAP to transport natural gas from Azerbaijan's Shah Deniz field. Moreover, he spoke of the challenges in building integrated transport delivery systems, which can cause problems further down the supply chain.

Tora Leifland Holmström concluded the presentations by explaining the Trans Adriatic Pipeline and its role in the southern gas corridor. She explained some of the factors consortiums like Shah Deniz look for when awarding contracts, including: commerciality, project deliverability, financial deliverability, engineering design, alignment and transparency, operability, scalability, and public policy considerations. Holmström also outlined some of TAP's key features, which will include an ability to supply 10-20 billion cubic metres of gas per year. It is also anticipated that TAP will have 80 percent physical reverse flow capacity, along with connectors linking it directly to TANAP.

Following the presentations, a lively discussion ensured between participants and speakers. A representative of the Albanian government, for example, spoke of the importance of major infrastructure projects to Central European countries, describing Albania's first cross-border pipeline as the most important infrastructure in Europe for years. Yet, another participant also pointed out that these decisions can sometimes create tensions between surrounding states because each is vying to become a regional energy hub. Dr Frank Umbach also intervened to point out how the ascendency of interconnectors helped changed markets that were previously nationally fragmented.

FIFTH EUCERS/ACATECH/KAS ENERGY TALK: TERROR ATTACKS ON ENERGY INFRASTRUCTURE - A GROWING THREAT?

The final EUCERS/ACATECH/KAS talk was held in October and examined the risks on energy infrastructure from terrorism. It explored whether the risks from this type of activity are growing and what steps can be taken to mitigate the associated risks.

The event included keynote speeches by Jennifer Giroux of the Centre for Security Studies (CSS) at the ETH Zurich, Dr Alexander Fekete, Professor of Risk and Crisis Management at the Cologne University of Applied Sciences, and Dr Frank Umbach, Associate Director of EUCERS.

Professor Dr Friedbert Pflüger, Director of EUCERS, chaired the session and recapitulated the current series of Energy Talks, of which the fifth session would be the last one for the year 2013. He stressed the importance to discuss the topic of attacks on energy infrastructure by referring back to the events earlier this year in Algeria, as well as the on-going problems in Nigeria regarding oil theft, and the Gulf of Aden regarding piracy. Hans-Hartwig Blomeier, Director of the London Office of the Konrad Adenauer Foundation, also gave thanks to the cooperation with EUCERS and held out the prospect of the upcoming series of Energy Talks, which will start next year.

Jennifer Giroux presented the Energy Infrastructure Attack Database that had been developed at CSS, which does not only include terrorism as a cause for an attack, but also piracy and insurgencies. By displaying the acquired data, she made evident how attacks on energy infrastructures have increased over the past 30 years, with repetitive peaks, constituting an average of 300-400 attacks a year. Ms Giroux stressed the importance that most of these attacks take place in clusters, implying certain regions with multiple attacks on similar targets. She presented the main geographical hot spots to be Iraq, Nigeria, Afghanistan, Pakistan, India, Columbia, Egypt, Syria, and Yemen. While cyber-attacks are of distinct interest for the centre, the difficulty of identification and attribution hinders an effective inclusion of this data. Finally, Jenifer Giroux displayed the centre's approach to

From left: Alexander Fekete, Friedbert Pflüger, Jennifer Giroux and Frank Umbach

utilise the contagion framework to explain the various factors leading to respective attacks, based on information on the agents, hosts, and environmental factors.

Professor Dr Alexander Fekete opened his presentation by questioning whether a high risk automatically implies a high probability. He then argued that by connecting an increased security to high risk targets, probability is decreased. He underpinned this theory through data on pipeline failures in the EU from 1971 to 2006, in which attacks and crime constituted only about 3%. By referring, however, to the 2006 Switch-Off that caused a black-out over half of Western Europe, Professor Fekete displayed the severe potential consequences of a well-targeted attack on the grid, making clear that the potential implications are as important as the degree of threat. The next question, therefore, was whether Europe is prepared to degrade gracefully, implying that not all parts of the system would shut down in the event of an attack. Based on a theoretical economic assessment in Germany, such preparation was considered to be present following a high degree of diversity and redundancy in energy supply. However, in practice not immediately considered potential targets of attacks on energy infrastructure, such as bridges, can have a severe impact on the security of supply. This is due to the fact that below most bridges run several energy distributors, such as gas, electricity, water etc. Finally, Professor Fekete pointed out the various interests and philosophies in crisis and risk management by various involved state agencies, which

Fluid Resiliency and Risk Management Culture: Emerging Security and Risk Perspectives for Dealing With Threats to Energy Infrastructure

BY ALEXANDER FEKETE

Fluid Resiliency of Attackers - Learning From an Unwanted Form of Resilience?

According to Jennifer Giroux, the CSS database shows that attacks on energy infrastructure are rising in various regions of the world. She emphasises this is a true trend, not just a bias of increased reporting. A specific characteristic is a trend in multiple and continuous attacks. For instance about 200 attacks in Colombia that show certain clusters and hot spot areas. Conceptually, the CSS uses, amongst others, a contagion framework that integrates the threat assessment with analyses of ethnology, social background and vectors of clusters of attacks. For instance, physical attacks in Colombia are rooted in communities, where groups form and continuously reshape - so called 'fluid communities'. This fluidity is based on changing and competing interests and interlinkages - political interests sit next to army & to crime. Physical attacks on energy infrastructure are just one mean of gaining income or power, emerging from actors deeply nested into their communities, exposing high level of flexibility to adapt to new situations or new security measures. In some sense, such actor groups exhibit a high level of what is commonly called resilience. This is possibly not 'resilience' in its usual positive connotation in the eyes of a gobal, public or energy producers. However, it showcases examples how the counter-reaction could be modernised to keep up with attackers; a more fluid and flexible type of security, with sustained and continuous efforts on learning and constant improvement, nested in communities and uniting interests of multiple stakeholders - ranging from the people striving for income, to political decision makers, army and others.

Is It All About the Threats?

The example of the attacks in Colombia already showed that analyses of growing threats on energy infrastructure couldn't focus on the threat/hazard side only. As in the case of the analysis of so-called natural disasters, both the threat and the impact side (adaptation, resilience, vulnerability) must be considered. For instance, the threat as counted by numbers of attacks in Europe might be very low as a study from 1971-2009 shows. However, pipeline interruptions are to a much higher degree caused by corrosion or human error. The threat is also composed of the fragility of highly interdependent infrastructure systems, as well as of the fabric of society and ecosystems that are impaired by such infrastructure failures or attacks.

Another possible conceptual trap in risk analyses is thinking high probability would equal high risk, deeply rooted in risk manager's minds and based on the oldest of risk assessments (insurance, military, engineering). It works for cases with a great number of observations, data-access and well-understood nature of threat without change. Intelligent attacks, however, work differently since saboteurs can actively exploit preparedness and security measures by circomventing or even misusing them.

A high number of continuous attacks should be a warning and set the focus on these hot spots. Nevertheless, a residual risk that this focus could be exploited, grows. As several cases showed (Mass shooting in Utoya, Norway, 2011, Spain 2004), double-attacks aim at redrawing resources or concentrating them in one spot just to place a second or third attack.

Focusing on the most valuable, critical or in other sense most obvious-for-attack asset could be misleading. These are often highly secured and it might be easier to select another target. So deriving risk management that measures a high probability of attack based on the value and therefore damage potential (cf. the typical risk matrix) can be misleading. This argument is quite ambiguous, since one shouldn't think that high security measures make a target unattractive per se. It can be highly attractive to demonstrate that especially those seemingly secure spots can be overrun.

Other aspects to consider are the intention and (risk) management of attacks. After one large terror event, it might not be necessary for the attackers to launch another succeeding large-scale attack. Smaller and more cost-effective actions might be enough to keep up attention.

This short paragraph is to outline the pitfalls in adopting traditional risk analysis concepts for intelligent attacks. There is ambiguity in the targets and ambitions of the attackers and in the counter-measures. Since the attackers are usually the ones planning the attacks, they are often more flexible and fluid than the security or response institutions. As in the case of the fluid communities of attackers in Colombia, it seems necessary to develop new security and risk concepts, for analysis as well as for management and governance.

New Fluid Security & Risk Governance Concepts

- *Do not just rebuild it (bounce back) but transform it and modernise it*
- *Build-in security into new infrastructure ('window of opportunity') & make this economically attractive, embed it in the community or overall system (make it sustainable)*
- *Develop new risk and resilience analysis methods - take care of unwanted side effects of resilience strategies and measures*
- *Keep fluid, keep on learning & changing*

However, there are at the same time certain caveats to address, such as the downsides of fluidity. Continuous, irregular change is a challenge for coordination and a sustainable use of resources. Diversification is to a certain extend connected to such fluidity - and decentralised insular energy producers such as households or small enterprises often have fewer resources or knowledge how to install and maintain IT security measures or conducting risk analyses themselves. Diversification of responsibilities is also a challenge for risk managers in a big company, since multiple departments order server and IT infrastructure, for example. It results in a growing lack of overview and coordination.

New Corporate Ethical & Sustainability Culture

New security concepts must be embedded into the existing strategy and culture of a community, company or any other user group. Take the oil spill in the Deepwater Horizon incident as an example. Was it a risk management responsibility, a risk communication issue of the top management or of the whole company culture towards security? The financial crisis in the US and Europe may serve as a similar example.

There appears to be a trend in the banking system to turn away from short-term strategies towards long-term sustainability. But how can this be manifested and managers convinced? By giving up bonuses? Or by increasing transparency of investments, such as in 'failed states' or in environmentally questionable projects? This would work only, if such measure were made obligatory to everyone. This could only work without regulation, when role models or 'change champions' with multiplier effects adopt such strategies in their company culture. In the banking system, certain banks, investment funds or other institutions (state pension funds) that are market leaders and therefore influential enough to make ethical and sustainability criteria in the selection of investments into projects so attractive and compulsory that other funding managers copy their strategy to stay competitive.

Critical Infrastructure Governance Versus Economic Trends

Economic interests are often not in favour of security topics, as they can be costly, time-consuming and hinder development. Therefore, it will take time to convince investors and politicians about the benefits of security and preventive planning. New technologies or development schemes can be a window of opportunity. But as experts in international relations, such as Frank Umbach, show: New risks turn up at the same time as new opportunities. For example, debates emerge about new unintended regulatory risks in Germany and Europe as a result of phasing out nuclear, embracing renewables and, some suppose, increasing the risk of blackouts. The trends in economy and modern technology are regarded more important than phasing out nuclear energy, demographic- or climate change, terror or crime, a survey (from 2011) among expert representatives of the infrastructure sectors in Germany has shown.

Resilience - a Rebounding or a Bouncing-Forward Perspective?

A lot has been written about the 'bouncing back' aspect of resilience - systems withstanding shocks more and recover more easily. Many recent crises have made us to reconsider, if it always makes sense to rebuild the same financial basis and trust in systems previously known as 'too big to fail' and to regulate large systems or even countries. Resilience is also a lot about flexibility, adaptive capacity.

The excellent summary on resilience aspects in energy systems by Friedbert Pflüger discusses the rebounding and the forward-looking perspective of resilience. From my limited experience in civil protection and risk research I would add to the 'Seven measures to build resilient energy systems' (Pflüger) that diversification and decentralisation (measures 1 and 2) are undoubtedly key ingredients of a modern take on stability of interlinked energy systems. However, one must also keep an eye on its limitations. Diversification can result in a loss of overview. Decentralisation can result in lower security standards, especially in smaller companies that are lacking resources and experience in risk management (see comments above). Preventive measures (measure 6) , also by the police and military, can face limitations in risks with a surprise factor. Prevention and planning are usually costly, time- and resource-consuming and often need to prove their benefits. This is why we urge for the development of criteria to evaluate the benefits and challenges of concepts such as resilience or vulnerability in an upcoming publication.

Finally, disaster control (measure 7) faces many limits, especially in policies on critical infrastructure protection. It has been recognised that a 100 % security promise cannot be fulfilled and should not be a goal. Rather, security institutions need to be embedded in society. And, customers of infrastructure services need to be made aware of pending risks. This does not mean that threats and intelligence information need to be communicated, but possible impacts and vulnerabilities. Security is often regarded as a counter player to freedom. Resilience still needs to show as a concept how these two worlds could be better integrated.

Footnotes: 1. German Federal Institute for Materials Research and Testing (BAM), Research Report (German) 285, 2009.
2. Source: Fekete, A. & Kraft, N. 2011, Infrastrukturen im Blick. Bedeutung, Trends und Bedrohungen aus Sicht von Branchenexperten. Bevoelkerungsschutzmagazin, Bundesamt für Bevoelkerungsschutz und Katastrophenhilfe, Bonn. (online at www.bbk.bund.de)
3. Pflüger, F. 2013. ENERGY SECURITY TURNS 100! Thoughts on resilient energy systems, energlobe.com, acessed 30 Oct 2013.
4. Fekete, A. & Hufschmidt, G. (forthcoming) Special Issue on Benefits and Challenges of the Concepts Resilience and Vulnerability for Disaster Risk Management, Int. J. Disaster Risk Science.

continue to hinder an effective assessment, preparation and mitigation of an attack.

Dr Frank Umbach concluded the presentations by explaining the challenges of energy security following the lines of diversification implying greater interconnectedness, and the security implications this interconnectedness has for physical as well as cyber-attacks. He argued that the increase in connectors following the 2009 gas blockade by Russia while having improved European energy security has opened new vulnerabilities with an increased cascading effect danger. Furthermore, cyber-attacks add the electricity grid to other high risk energy infrastructures, such as oil and gas. This is of particular importance for critical infrastructure, as in hospitals, and renewables. Dr Umbach further elaborated how the new dangers of the cyber world threaten developed states, as both power plants and critical infrastructure share two common features, which are their dependence on electricity, and the connection to the internet. This becomes all the more alarming since there is no experience in dealing with such new threats, and businesses, who have become victims of cyber-attacks or blackmailing have had a distinct interest in not publicising information in this regard. With respect to preparedness, Dr Umbach stress how the false feeling of security has enabled the attack on the Algerian power plant earlier in 2013, and pointed out the lack of awareness and acknowledgment by company leaders of security threats, which are not considered a business priority. Moreover, smaller companies will not be able to provide the funds for adequate security provisions, which decreases their presence in unstable regions with potentially severe repercussions regarding needed investments in new energy infrastructures for the future. Finally, Dr Umbach concluded that there is the need for a change in security culture in companies, reaching all the way up to the CEOs, with a distinct focus on mitigation and recovery, not just prevention and preparedness.

Following the presentations, a lively discussion between the participants and speakers

From left: Hans-Hartwig Blomeier, Friedbert Pflüger and Alexander Fekete

developed with critical views expressed about the points made. One question for example focused on the difficulty that short-term stakeholder commitments entail with regard to a change in a company's security culture. Professor Pflüger drew the attention again to the increase in physical events, focusing on the developments in Nigeria, where oil theft becomes an increasing problem.

A new emphasis was laid on the root causes for violence, which can only be targeted by companies and states together within the respective communities, as well as on the danger of attacks on Nuclear power plants. The panel gave founded arguments to all posed questions, and pointed out with regard to the last one that nuclear power plants are among the most secure energy infrastructures, and a far greater risk and probability lies in an attack on LNG terminals in harbour cities, which could have a destructive effect similar to a tactical nuclear bomb.

IV. Summary

The EUCERS/ACATECH/KAS series on energy resilience at King's College London spanned several months and brought together a range of different participants who are concerned about the future of energy policy. Over five different workshops an authoritative perspective was provided across a range of topics with input from policy experts, academics, students, and industry representatives.

Participants were agreed that achieving a resilient energy infrastructure must be a priority for European governments over the coming years. Moreover, there was a broad consensus that no one party would be able to achieve this alone, and that greater cooperation would be needed between governments and the private sector. In particular the former would need to intervene in the market to provide some protections and incentives, to encourage the latter to invest in research and innovations.

It was also felt that innovation should be just one part of the strategy. Resilience would also need to be achieved by mitigating risks, forward planning, and diversifying the energy mix as widely as possible.

The EUCERS/ACATECH/KAS Energy Talks were organised by the European Centre for Energy and Resource Security, in conjunction with ACATECH – the German National Academy of Science and Engineering – and the Konrad Adenauer Foundation in London. The events were all held at the Strand Campus of King's College London.

The aim was to foster critical dialogue and creative thinking in a neutral environment among different parties. The series also led to increased awareness around the issue of resilient energy infrastructures. With high attendance at all events, and positive input from participants, these aims were achieved.

We would like to thank all keynote speakers, commentators, and participants who contributed to the success of the round-table discussions while enriching our understanding of the subject matter.

APPENDIX

V. List of EUCERS/ACATECH/KAS Energy Talks

Energy Talk 1 – 12.3.2013

Europe's Vulnerability to Energy Crises

Purpose of workshop: to provide a general assessment and overview of the issues surrounding energy resilience and its significance. This will set the tone for the workshop series, by establishing the importance of the series and explaining the key issues we hope to explore in coming weeks, while offering a general primer of the key points. *Keynote Speakers:* Dr Frank Umbach, Associate Director, EUCERS, King's College London, Dr Thomas Rid, Reader in the Department of War Studies at King's College London and a non-resident fellow at the School for Advanced International Studies, Johns Hopkins University, in Washington, D.C.

Energy Talk 2 - 8.4.2013

Building Resilient Energy Infrastructure Beyond Europe's Borders.

Purpose of workshop: to explore what coordinated European action can do to promote resilient infrastructures in developing economies which are subject to regular bouts of political unrest. This would allow us to explore, for example, what impact the Arab Spring had on energy concerns in Europe, and what best practices might be developed going forward in order to counter such challenges. *Keynote Speakers:* Prof. Dr. Klaus Thoma, Head of the Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute in Germany and member of the German National Academy of Science and Engineering (ACATECH). Yolanda Garcia-Mezquita, Internal Market II: Wholesale markets; electricity & gas, DG Energy, European Commission.

Energy Talk 3 – 3.5.2013

The Danger of Blackouts - Electricity Security as the Achilles Heel of Resilient Energy Infrastructure?

Purpose of workshop: it is often said that securing electricity security should be the most important priority for Western governments because it can be produced from a wide variety of different sources, insulating it to disruptions against any single source. This workshop explores whether resilience of electricity infrastructures should be prioritised. If so, why and how? What challenges will it face and what practical steps can be taken to achieve this? *Keynote Speakers:* Jörg Asma, Partner KPMG and member of the Resilien Tech Working Group, ACATECH – National Academy of Science and Engineering, Germany. Dr Sarah Mander, Deputy-leader of the Tyndall Energy Programme, Tyndall Centre, Manchester University.

Energy Talk 4 – 18.6.2013

Challenges and Prospects for an Integrated Energy Infrastructure in Europe

Purpose of workshop: to discuss what has gone right – and what has gone wrong – with integrated energy plans in Europe. What might greater cooperation look like in the future and how should it be promoted? This workshop will also explore challenges to greater cooperation and discuss how pan-European risks can be mitigated.
Keynote Speakers: Dr Anita Orban - Ambassador-at-Large for Energy Security, Hungary. Thomas J. Dimitroff, Partner, Infrastructure Development Partnership, LLP. Tora Leifland Holmström, Government Affairs Advisor, Trans Adriatic Pipeline (TAP).

Energy Talk 5 – 31.10.2013

Terror Attacks on Energy Infrastructure – A Growing Threat?

Purpose of workshop: this workshop will focus on the risk of terror attacks on energy infrastructure. It will discuss terrorist attacks such as the incident at the In Amenas gas facility in Jan 2013 and analyse if attacks on energy infrastructure present a growing threat. *Keynote Speakers:* Jennifer Giroux, Centre for Security Studies, ETH Zurich, Switzerland. Dr Frank Umbach, Associate Director, EUCERS, King's College London. Professor Dr Alexander Fekete, Risk and Crisis Management, Cologne University of Applied Sciences/FH Köln.

IMPRINT

Publisher
Konrad Adenauer Stiftung
63D Eccleston Square
London SW1V 1PH
United Kingdom
Phone +44 20 783441-19
Fax +44 20 783441-34
E-mail: kas-uk@kas.de

Tiergartenstraße 35
10785 Berlin
Germany
Telephone: +49 (0)30/26996-0
Fax: +49 (0)30/26996-3261
E-mail: redaktion@kas.de

Coordination and Editing
Carola Gegenbauer
EUCERS, King's College London
Department of War Studies
Strand, London WC2R 2LS
United Kingdom
Telephone: +44 (0)20 7848 1912
Email: info@eucers.eu

Design
The Color Company
Suite A, 1 Lindsey Street
Smithfield
London EC1A 9HP
Telephone: +44 (0)20 8900 4164
Email: design@color.co.uk

Photo Credits
Carola Gegenbauer, EUCERS, King's College London

www.kas.de

www.kas.de