WORKING PAPER [4]

JUNE 2012

Enhanced Resilience Through Innovative Networked Security

Dr. Boaz Ganor (International Institute for Counter Terrorism; Lauder School of Government, Diplomacy, and Strategy, IDC, Herzliya)

Dr. Markus Hellenthal (Germany)

International Institute for Counter-Terrorism (ICT)

Additional ICT resources are available on ICT's website: www.ict.org.il

About the Authors:

Dr. Boaz Ganor is the Ronald Lauder Chair for Counter-Terrorism, the Deputy Dean of the Lauder School of Government, the founder and Executive Director of the International Institute for Counter-Terrorism (ICT), and the head of the Counter-Terrorism and Homeland Security Studies Programs (Graduate degree, Executive program and Bachelor specialization) at the Interdisciplinary Center (IDC), Herzliya, Israel. He is also the founder and President of the International Academic Counter-Terrorism Community (ICTAC), an international association of academic institutions, experts, and researchers in fields related to the study of terrorism and counter-terrorism.

Dr. Ganor is a member of the International Advisory Council of the International Centre for Political Violence and Terrorism Research at the Institute of Defense and Strategic Studies (IDSS), Nanyang Technological University, The Republic of Singapore. He is also co-founder of the International Centre for the Study of Radicalization and Political Violence (ICSR), a partnership between the University of Pennsylvania, USA; the Interdisciplinary Center, Israel; King's College, London; and the Regional Center on Conflict Prevention (RCCP), Jordan. Dr. Ganor was a Senior Fellow at The Memorial Institute for Prevention of Terrorism (MIPT), Oklahoma City, USA; and was a member of the International Advisory Team of the Manhattan Institute (CTCT) to the New York Police Department (NYPD).

Contact email: ict@idc.ac.il

Dr. Markus Hellenthal designs and implements innovative and competitive solutions in the field of, among others, mobility, security and defence and has achieved significant sales successes in Germany, in Europe and internationally. He has gained in over 25 years an exceptionally broad professional experience in senior executive positions, the first half in the public sector and the second half in the private sector. In his last position as Senior Vice President of the Thales Group and as Chief Executive Officer of Thales in Germany he was accountable for 7,500 employees and 1.4 billion Euro sales as well as member of the supervisory boards of ESG GmbH, Diehl AirCabin GmbH and Diehl Aerospace GmbH. Prior to that he was Senior Vice President of EADS (today Cassidian) and a Partner of Accenture. Before that he was law enforcement officer and Government official in North Rhine Westphalia and with the federal government administration, his final position being Director Federal Border Police. His competences focus specifically in strategic business development and change programs as well as capability increases enabled by latest information and communication technologies. Since more the last 10 years he is involved in the European and German security research agendas and is consulting German and international enterprises as well as the German Federal Ministry of Economy and Technology.

Abstract:

The article begins with an introduction of the new security challenges in the globalization era and illuminates the vulnerability of modern societies. Dr. Boaz Ganor and Dr. Markus Hellenthal further state the intrinsic connection between crime and terrorism and advocate a new approach regarding a more advanced security system that takes advantage of a networked world. They criticize the existing segmentation of the security sector and argue for efficiency in security obligations through a better integration of different internal and external networks. In addition, Ganor and Hellenthal propose that an enhanced productivity of security in the matter of an upgraded and interconnected information and communication technology would enable to integrate and improve performance. Ganor and Hellenthal conclude with a number of suggestions for different forms of additional security technology with the underlying purpose of keeping a balance between individual civil rights and collective security needs.

Enhanced Resilience Through Innovative Networked Security

Dr. Boaz Ganor (International Institute for Counter Terrorism; Lauder School of Government, Diplomacy, and Strategy, IDC, Herzliya)

Dr. Markus Hellenthal (Germany)

[The article begins with an introduction of the new security challenges in the globalization era and illuminates the vulnerability of modern societies. Dr. Boaz Ganor and Dr. Markus Hellenthal further state the intrinsic connection between crime and terrorism and advocate a new approach regarding a more advanced security system that takes advantage of a networked world. They criticize the existing segmentation of the security sector and argue for efficiency in security obligations through a better integration of different internal and external networks. In addition, Ganor and Hellenthal propose that an enhanced productivity of security in the matter of an upgraded and interconnected information and communication technology would enable to integrate and improve performance. Ganor and Hellenthal conclude with a number of suggestions for different forms of additional security technology with the underlying purpose of keeping a balance between individual civil rights and collective security needs.]

Introduction

Human life is constantly challenged by many uncertainties of all types and magnitudes, as is nature at large. Security is thus relative, and is influenced by geographic, sociological, societal and legal factors, but also many other interrelated aspects, such as

health, family and labor relations, criminality, man-made and natural disasters to name just a few.

Not only since September 11, 2001 - security is thus ultimately an exceptional situation we strive to achieve, and effort and expense are required every day to establish and maintain it at the desired level. Increasing globalization demands even more energy for tackling the manifold and interlinked issues with which modern societies have to deal with with regards to security, rule of the law and freedom; that is, it demands transnational legal and legitimate cooperative cross-border action in all areas, whether it is from business, governmental or cultural perspectives. At the same time, we are experiencing the almost daily introduction of ever-faster developing technology in many areas of our lives. The new capabilities ultimately help all players, unfortunately including the illegal and criminal ones.

Globalization increases worldwide capital and goods movements, information and knowledge exchange and urbanization, as well as migration due to climate change, scarcity of resources and globalization of also the labor market. According to UNHCR, the United Nations High Commissioner for Refugees, nearly 45 million people are fleeing today from somewhere[i].

On top of that, we have natural catastrophes and major incidents such as pollution of the Gulf of Mexico, flooding in Australia and the catastrophic domino effect of the earthquake, tsunami and the near nuclear meltdown in Japan. These incidents, together with the growing dangers posed by cybercrime, dramatically demonstrate how vulnerable modern societies have become and how vital all-encompassing protection of assets such

as critical infrastructure now is. Additionally, these threats transcend national borders and existing organizational structures. They also confirm that the old distinction between symmetric and asymmetric threats is no longer helpful in today's world; in fact, it sometimes hampers proper and efficient action.

Terrorism and Crime

There is another essential dimension, which cannot be tackled using the traditional silo approach. This is the interdependency, or rather integration with globalization, of terrorists and other organized criminals. An example of this growing phenomenon is the prominent involvement of terrorist organizations in the production and distribution of drugs and their correlation with all kinds of enabling criminal activities and shadow facilitators, like money launderers, weapon and alien smugglers, counterfeiters, etc. This also means that terror organizations become more and more independent of state support or subsidies and become businesses of their own. They follow their own agendas, which makes them even more dangerous to the free and democratic countries. They use regular transportation means like containers and ships, as well as latest communication technologies.

This presents a dilemma that has been with us throughout mankind's history - from the first Stone Age hand axe to today's nuclear technology and the Internet. Everything has two sides. On top of this dilemma there is a technological competition between the state security apparatuses and terrorist and criminal organizations. Each one is trying to be ahead of the other. New criminal and terrorist techniques promote the development of new technologies that will help the police and security services to contend with the new

challenges. The new technologies are posing new obstacles to the terrorists and the criminals and force them to develop new modi operandi or to use new technologies by themselves. This technological race leads sometimes to the use of more lethal weapons and creates a dangerous paradox. The twentieth century has gone down in history as the century of – hopefully - the last conventional wars as addressed by the Hague Conventions. We are now already in a century of asymmetric threats that do not comply with any international rules. Terrorism is neither a new nor only an Islamist phenomenon. However, given the tactical and technological capabilities available today, it has entered a totally new dimension and is thus a much greater threat to our societies.

These threats are not isolated, stand-alone incidents, nor can they be tackled separately and consecutively. On the contrary: We are faced with potentially tremendous damage and loss, which can grow out of patterns of interdependence. They stop neither at national borders nor at the boundaries of traditional organization charts of civil or military security organizations.

Security in a Networked World

The world over, these threats have changed the perception and the understanding of security and the importance of the resilience of modern societies at large, as well as of companies and even individuals. In order to support our common endeavor to defend the shared values of our countries from terror and other criminal acts, societies must guarantee the availability and integrity of their diverse security and resilience capabilities at large.

Such security providers include law-enforcement authorities, fire departments, civil defense organizations, search & rescue organizations, and others, including military resources if necessary. The latter is especially important with regard to logistics support, heavy vehicles or construction, engineering, decontamination and similar capabilities, which are otherwise attached and attributed to the military. Security providers are also private security companies or operators of critical infrastructure like ground and air transportation systems, harbors and associated industrial sites. It is well known that over 80% of critical infrastructures are owned or operated by private companies.

Security and mobility in a networked world are thus among the key challenges governments, industry and research institutes must address in the twenty-first century.

In essence, whether we are confronted with symmetric or asymmetric criminal or terrorist threats, our ability to prepare and respond adequately depends essentially upon our ability to take the necessary actions, especially toward unplanned disruptive challenges. Such actions rely on adequate risk management procedures and techniques to anticipate, detect, identify, analyse and mitigate relevant threats appropriately, decisively and effectively.

In the following, I would like to ask some questions to address potential for improvement:

New Challenges of Responsibility

Question 1: How can our various human communities, be they local or international, handle existing insecurities and threats without becoming paralyzed or panic-stricken? Or in other words: How do nations satisfy the legitimate need of their citizens to avoid on

the one side terrorist acts and other criminality as well as scenarios such as the recent ones in London on the other side?

Without wishing to expound on the philosophies of Hobbes or Rousseau, one thing should be clear: When, based on the rule of law, a national monopoly on the use of force ceases to exist for whatever reason, we will no longer have a state of "free love" simply one ruled by the rights of the strong. And the strong are not the upright citizens, but gangsters, pimps, dealers or terrorists, especially when they are equipped with modern offensive and defensive technical means and organize themselves via social networks or similar.

It would be remiss to discuss global terrorism without also mentioning the local aspects of security. The first and foremost task of policing is to guarantee that citizens are secure at home and at work and that no criminal actions are conducted against them or the society. It is basically all about prevention; response and recovery are only an unfortunate proof that prevention was not successful.

This assumes that those responsible on the ground know the people and their local situations, prevent crime and threatening situations by sensitizing and communicating with the people in the community, helping to keep them safe from day to day. Without a visible police presence in the public arena and without a trusting relationship between the police and the citizenry, there is no such thing as lasting inner peace in a democratic society. Wherever this link is broken, fertile ground is established for criminality through terrorism in parallel with the growing doubt in the state's ability to keep the peace internally. Ultimately, the monopoly on the use of force weakens and the right of the

strong begins to take over. Both organized crime and individual suicide bombers need an extensive network of either active supporters or passive suppliers or just knowledgeable bystanders. The closer the police are to the pulse of the people and the more intimately they work with other security organizations in an integrated manner, the greater is their daily contribution to peace and to the general security of a democratic society.

So the alleged contradiction between inner peace and security really does not exist. Instead, this ideology aims to eradicate the democratic state by withdrawing one of its core duties, which is to exercise its monopoly on the use of force to maintain the rights and freedoms of its citizens. This guarantee of democratic rights applies to all citizens within the respective nation's jurisdiction, regardless of skin color, religion, level of education, place in society, sexual orientation, how large their bank account is, or whether they even have one.

A modern state that does not wish to abdicate its duties must maintain the peace and guarantee freedom within its entire area of responsibility. When conditions change, this means nothing more than adjusting to new challenges and responding accordingly.

No private organization would do anything less. If financial limitations exist, as is the case in times of escalating national debts, priorities must be established and areas identified where costs can be reduced without compromising the guarantee of democratic rights.

Efficiency in Security Obligations

Question 2: Why are internal and external security usually still regarded separately? In terms of the democratic state's monopoly on the use of force and its duty to guarantee

safety and in view of overwhelming asymmetric threats, is it not downright antiquated to separate allegedly pure military competences from allegedly pure policing proficiencies?

Or, more generally speaking: Had we known about the myriad threats we currently face and the capabilities available to and required by a state to fulfill its security duties, would we have created the fragmented and silo-like organizations that often exist today?

Even established traditional, clearly time-tested structures and architectures have a best before date and should subsequently be replaced by something new. At some point in time, the cost of maintaining the old exceeds that of replacement. In my opinion, some of what we call the security architecture in our countries falls under the heading "established tradition." Some of it can only be explained historically, and is furthermore extremely expensive. This applies for example to the separation of military, police - vertical and horizontal - and many other security organizations in view of the fact that there is really no longer any difference in their mandates. Conventional wars in terms of the Hague Conventions basically no longer exist; neither in Afghanistan nor in seaborne anti-piracy missions. There is broad consensus that what we see there is rather a striking lack of internal peace, which cannot be effectively countered with normal policing means based on everyday policemen and policewomen walking the beat. However, typically most police forces do not have the required resources, whereas military organizations have them, but are often not permitted to use them; or, even worse, the military capabilities have been designed for classical naval war theatres and not to current piracy attacks.

What is also missing is integration or end-to-end networking with all the other security organizations such as fire departments, emergency services, disaster control, private security providers etc.

This is not intended to diminish the undeniable successes of today's civilian and military security organizations, or to criticize the improvements being made everywhere. But perhaps we would be even better equipped for the future if we were to take the commonsense approach of the head of a family or CEO of a company to thoroughly revamp our structures here and there. The route to take would normally be quickly found: Efficient use of resources by allocating resources according to need without taking into consideration traditional organizational boundaries. A shared service is the approach of choice, even when it comes to guaranteeing security.

By no means am I questioning the existence of federal state structures, or nation states at large. But I am firmly convinced that within the existing state structures, we do not need to establish and finance umpteen independent entities and capabilities, and then operate them independently of one another. More efficient - that is, more productive and cost-effective - ways exist for a state to fulfill its security obligations, which then will presumably also deliver better results in terms of higher productivity.

I would like to demonstrate the problem by providing just one example: There are cities or countries in which very similar security organizations exist immediately adjacent to one another. For a typical city in a typical country you have:

- community police
- provincial police

- federal police
- military security organization
- public railway security organization
- international airport security organization
- oil refinery security organization
- chemical industry security organization
- customs
- fire department
- coast guard
- search and rescue services
- national transportation authority's traffic control center

Of course each of these services has its own situation and central command center, its own mission control organization and its own information and communication infrastructure. This represents at least 100 security employees per city that could be redeployed just in the situation and central command centers alone without impacting efficiency negatively. On top of that, infrastructure and operating costs would be cut drastically. There are many other examples where creating and using shared centers of expertise would not only lead to significant savings, but also dramatically improved professionalism and greater productivity.

All of these are ways to get more “bang for the buck”, to cite Robert Gates, the former U.S. Secretary of Defense. In view of the existing threats and significant budget restrains, efficient and intelligent utilization of resources is called for, and should not be sacrificed

on the altar of allegedly sacred cows. If we continue to do so, it will be harder in future to explain to taxpayers, why.

But what is even more problematic, is the possible loss of productivity and mission efficiency:

- How much data and information get lost or arrive too late because of the lack of integration and seamless cooperation of security organizations?
- How many operations could be conducted faster or more effectively if the relevant security organizations were working
    - with an integrated situation and command center
    - in a real integrated fashion that transcend existing geographic and organizational borders
    - instead of side-by-side - or sometimes maybe even somewhat in competition?

Enhancing Information and Communication Structures

Question 3: Which technical improvements are called for in order to enhance the productivity of security provision by states and the efficiency of command and control?

- Are the security organizations in their need to seamlessly collaborate with each other supported by the appropriate information and communication technology systems?
- And, if so, have they access to adequate real time sensing and decision support systems?

- And, if so, are these embedded in inter-organizational processes and alarm systems?

With the right information and communications technology, efficiency and productivity can be increased significantly. Even today, individual security organizations buy, develop and maintain countless redundant IT systems for reasons of pride and vested interests. Islands even exist within individual organizations, which IT companies like to take advantage of, but overall are a waste of taxpayers' money. IT is often seen, even today, as a way to speed up established, traditional ways of doing things. But maybe we no longer need these old processes at all; or at least, not the way they were devised by experienced administrators twenty or more years ago.

Sometimes even a lot of money is thrown at special technology gadgets which are standalone and cannot be integrated in the larger system architecture.

IT is first of all an enabler of efficient ways to integrate and improve performance. This applies not only to industry, but also the government, especially security organizations.

The aim of integration is to give security organizations and their personnel access to operational tools that give them clear, comprehensive situational information, enable them to interact quickly and easily with the public while coordinating with other security forces and ultimately, to make an appropriate decision about what is required to cope with the situation at hand and then execute the necessary steps.

In addition to the integration and distribution of information, the principle of recursion, or self-reinforcement, is a key element of prevention and response. Individual actors can

only contribute to the self-reinforcement of the entire system when they are bidirectionally tied into the overall communications process.

This means that:

- The various bits of information from different sources are merged in real time to give security organizations working in concert a common understanding of the situation.
- This information is made available again in real time to the teams from various organizations working in concert in order to improve mission efficiency in a global, networked environment.
- The information from the task forces is fed back in real time into the overall situational analysis in order to continuously expand and improve its quality.

Ultimately this means that all actors are living with the same situation. The described self-reinforcement is thus the key to successful prevention and response. It leads to significantly improved operational execution as a result of the expanded potential capabilities.

This holistic approach creates a networked security system from the classic information gathering and communications structure, from the situation and command center to the various task forces that to date have not been seamlessly networked. The situation and command centers, participants, as well as sensors and optronics for data acquisition are all bidirectionally linked with one another. Diagrammatically this means that instead of a horizontal tree structure, we have a star whose points are linked.

Additional Security Technologies

Question 4: What additional technologies are needed to support the required integrative and holistic approach for providing security?

In general, providing security is all about comprehensive situational awareness of what is going on, achieving a constant scenario based understanding of what might happen, and what has happened in case of a security relevant event. This leads to some specific future technological needs in certain areas:

Protection of critical infrastructures etc.: Apart from material or smart or virtual fences, access control with biometrics to sensitive areas and monitored protection from forcible entry, C2, sound, image and radar networked sensors, including CBRN, the sensor analytics and management capabilities are the most challenging elements today. It is about being comprehensive and fast, encrypted and reliable and to be able to share the right information with the relevant forces and decision makers and from them to dispatch decisions effectively to any responding forces.

Urban security: The aerial dimension is relatively weak in the urban regions (for observations and reconnaissance missions) and there is a great need to efficiently compress data (especially video) and transmit it to mobile units. For the local security organization the challenge is not only to know first but also to decide first and to act first, including comprehensive coordination and cooperation. Therefore the traditional unidirectional communications system should be replaced by bidirectional communications, including handling of sensors; this means, the sensitivity and orientation of sensors can be defined by central command or the task force itself can

transmit video images to the command center. At the same time, the task force can also directly communicate with the sensor system and can analyze video images from nearby cameras without involving the command center.

Transportation security: While perimeter security is relatively effective, there is primary need for technology solutions for securing mass transportation at large. Outside aviation security, this topic has not been looked into comprehensively. In aviation security there is obvious need for applying more risk management approaches to improve passenger flows without compromising security, starting from what IATA has initiated already in the beginning of the 90th of the last century.

Visual Intelligence: The current capabilities (including the use of 3-D modeling, virtual and expanded reality) are admirable but not sufficient since they can cove a narrow area and need to follow a concrete target or trail of intelligence. It is like looking at the ocean through an old captain's telescope: he can only see one vessel at a time and cannot really understand the vast naval picture. It creates many operational dilemmas and weaknesses. The current challenge is how to be able to create a comprehensive picture of large areas (i. e. a city) continuously and with high resolution. It will provide a library of the area activities and any intelligence research, operational planning or even a crime investigation will be able to dig inside this library backward, as much as needed, to identify and track the needed information.

Signal intelligence: Organized criminals and terrorists are putting enormous efforts in avoiding the Sigint (signal intelligence) and Commint (communication intelligence) nets of the security organizations. This is in principle not new, but the technological

development is fast and the challenges on the side of the security organizations are increasingly demanding. The goal is for them to be able to identify, merge and exploit in very short time frames of seconds signal content of a possible target from different platforms of encrypted communication (SMS, chats, cell phones, web activity), to fuse these data, to mark patterns and links and take adequate action if need be even though the opponents take enormous precautions.

The field of **cyber-attacks** and **money tracking tools** (to block the flow of financial) are also growing needs for technologies.

Border control (land, sea and air): There is a growing need to be able to identify forged or falsified documents (to intercept illegal or covered traveling and movements) and to scan quickly and easily cargo for contraband (man, weapon and drug smuggling).

Long distance bomb disposal: The emerging challenge of suicide attacks pose the need to identify explosives from distance and to neutralize them from distance, without risking the life of the security personnel and police officers that today need to approach the suspect and be in his immediate proximity in order to search him and to neutralize the explosives.

Non lethal weapons: The danger in having false positive identification of a suicide attacker might lead to the killing of an innocent suspect. Therefore there is a need to develop a new and efficient non lethal weapon that will secure the life of a person who is mistakenly being suspected as a suicide attacker.

In conclusion, one comment is particularly important:

When establishing and operating efficient security architectures, we must never lose sight of keeping a balance between individual civil rights and collective security needs. Security cannot be seen as a threat, but is the basis of a free community.

[i] http://www.unhcr.org/pages/49c3646cbc.html