September 2016

THE KOSCIUSZKO INSTITUTE

THE KOSCIUSZKO INSTITUTE POLICY BRIEF

Joanna Świątkowska, Magdalena Szwiec, Ana-Isabel Llacayo

"Make a Bomb in the Kitchen of Your Mom" – How Terrorists Use Cyberspace and How to Fight with Them

authors

Joanna Świątkowska – Ph.D., is the Programme Director of the European Cybersecurity Forum, the Chief Editor of the European Cybersecurity Journal, Senior Research Fellow of the Kosciuszko Institute.

Magdalena Szwiec – Junior Research Fellow of the Kosciuszko Institute, graduated with a Master's degree in International Relations, scholarship holder from Tel Aviv University, Oslo University and Siena University.

Ana-Isabel Llacayo – Junior Research Fellow of the Kosciuszko Institute, holds a double Master's degree in European Politics with a specialization in European Security and International Stability from the Strasbourg Institute of Political Studies and the Center for European Studies at the Jagiellonian University in Kraków.

The Internet is a double-edged sword. Like most modern inventions, it has the potential to bring progress and improvement, but also carries with it negative consequences. The "dark side of the web" appears in many different ways and serves as a tool to achieve the goals of various actors – criminals, hostile countries and increasingly terrorists.

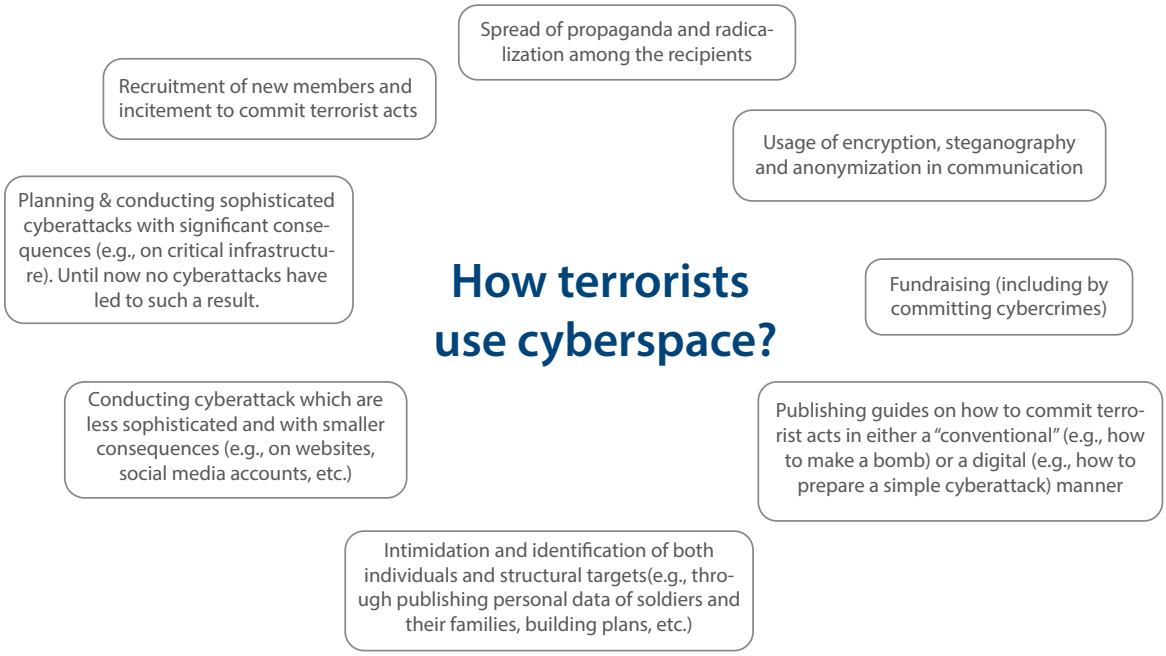
Terrorist groups and lone-wolves recognized this "advantage" of cyberspace, and they use it in a multitude of different ways. It is one of the biggest threats which the international community faces. However, every coin has two sides, and the Internet gave completely new opportunities for those who combat terrorism.

The goal of this policy brief is not only to introduce selected methods in which terrorists use cyberspace, but also to present a brief overview of the activities undertaken by security agencies.

What is the real picture of the threat?

Terrorists very easily adapt their methods to the conditions in which they are functioning. They change tactics, look for new opportunities and tools which may enable them to achieve a set goal. The internet brought a broad spectrum of possibilities in this

ISSN 1689-9873



regard. Terrorist groups, like Al-Qaeda, for years have taken advantage of the opportunities which the Internet provides. They were using it as early as in the '80s, mainly for propaganda.[1] The Internet was also an important tool used while preparing the attacks on 9/11, specifically to communicate, plan and obtain financial support.[2] However, while terrorists have used cyberspace to undertake their actions for a long time, the last few years have shown a significant growth in this phenomenon. The graph above shows how and why terrorists explore the web.

Even though terrorists have made attempts to conduct cyberattacks on targets that can be considered as critical infrastructure, until now these attempts were unsuccessful. Hence, until now we have not experienced spectacular cyberattacks that would cause harm in the real world, which then could be defined as cyberterrorism.

For now, cyberspace is mostly used as a supporting tool for "conventional" activities. For instance, terrorists use cyberspace to communicate, gain financial aid, spread propaganda or to share instructions on how to conduct an attack. In the web, terrorists publish "guides" which explain how to prepare the tools necessary for an attack. "Make a Bomb in the Kitchen of Your Mom" may serve as a perfect example of such a publication, describing how to make a homemade bomb. Other examples could be *The Mujahideen Poisons Handbook*[3], a guide on how to prepare a poison, or *Encyclopedia of Jihad,* were several chapter are dedicated to teaching how to kill someone. Furthermore, terrorists use the Internet to find information about objects and entities which they are interested in. They openly declare that the web and its open sources allows them to get access to approximately 80% of the information about a set target[4]. Such information is later successfully distributed. Not so long ago, terrorists were able to share a list of names of approximately 4,000 people through the use of a specially dedicated app who in the name of revenge should be eliminated[5]. These action effectively support the actions of "lone wolves", who having been inspired and helped by the provided information conduct attacks.

Experts claim that the main reason for which terrorists use supportive means more often than actual

1 J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad*, Institute for Critical Infrastructure Technology, 2016, pg.5.

2 United Nations Counter-Terrorism Implementation Task Force, *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*, UN, 2011, pg. 1.

3 Ibidem, pg. 20.

4 Ibidem, pg. 20.

5 Mirror, *ISIS 'Kill List' Names Brits Among 4,000 Terror Targets It Threatens to 'Kill Strongly'* in *"Revenge for Muslims"*, http://www.mirror.co.uk/news/world-news/isis-kill-list-names-brits-8271912, (access: 30.08.2016).

cyberattacks is a lack of knowledge and skills which would enable them to plan spectacular and sophisticated actions. Nevertheless, these circumstances could rapidly change. First of all, there is a possibility that among many of the new recruits of terrorist groups are people who poses advanced technological knowledge and skills. Secondly, the black market is dynamically growing (Crime-as-a-Service), and both the information and tools to prepare an attack are easily accessible. All this causes an expansion of the threat, and the vigilance of states should not get weaker.

The interest of terrorist groups in better organized actions in cyberspace is growing significantly. They create their own specialized "divisions" which are responsible for operations on the web (e.g., Al-Qaeda and its Qaedet al-Jihad al-Electroniyya),[6] along with a set of groups unofficially supporting them. Lately, a lot of new groups which mainly support the so called Islamic State have arisen (e.g., Caliphate Cyber Army, Islamic State Hacking Division, United Cyber Caliphate, etc.).[7] These groups exhort carrying out a so called cyber-jihad.

Many fronts of the fight against terrorists

In the near future an exploitation of cyberspace by terrorists might become one of the biggest threats for international security. When the center of gravity will shift from supportive actions to operations of more strategic means (e.g., serious cyberattacks on critical infrastructure), the consequences could be dramatic. That scenario is even more dangerous than the potential use of offensive capabilities by state-actors, which naturally take actions which are more rational and accurately calculated. In this regard, terrorists have nothing to lose as they are not afraid of conflict escalation or retaliation. What matters for them is causing as big of loses as possible. The unpredictability of their actions and their lack of inhibitions makes the scenario of a cyberattack conducted by them one of the worst possible.

That threat has been already noticed by the relevant players, who undertook concrete actions in response. As an example, the US Secretary of Defense announced in April 2016 that USCYBERCOM was ordered to use offensive cyber capabilities against the so called Islamic State.[8] A digital response does not eliminate the use of conventional means. Hence, Junaid Hussain became the third most wanted person on the list of entities combating the organization and was killed by a drone strike.[9]

Paradoxically, the fact that terrorists are increasingly using cyberspace also provides new opportunities in order to combat them. In this regard, law enforcement agencies responsible for security issues more often combine traditional investigative methods with new types of actions adequate for a digital environment. Thus, they are able to counter terrorist groups, to thwart their plans and to arrest suspects in a way which was impossible in the past.

In the face of the latest numerous terrorist attacks, consecutive countries introduced new or improved their current legal regulations which aim to strengthen and expand a set of tool available to combat terrorism. Besides more conventional measures, new counterterrorism strategies emphasize the mechanisms that enable law enforcement agencies to act more effectively in fighting terrorist actions in cyberspace. That trend is accompanied by a broad discussion about the efficiency of the tools used, as well as the possible side effects on the abidance of human rights (especially the right to privacy).

In view of the form and nature of this publication, we will not elaborate more on these matters. We will focus on particular actions undertaken lately by selected states. Doing so will allow us to identify leading trends in those countries and might be used as a material for discussion about those mechanisms which were implemented. To become more familiar with the original information about how these concrete tools are used (conditions, circumstances and all other details), we encourage the reader to look at the reference text. Below we introduce the information in a simplified manner.

6 J. Scott, D. Spaniel, *The Anatomy of...* op.cit., pg. 6.
7 More: J. Scott, D. Spaniel, *The Anatomy of...* op.cit., 2016.
8 J. Scott, D. Spaniel, *The Anatomy of ...* op.cit.,. 23.
9 Ibidem, pg. 15.

COUNTRY	TOOL/POWERS INTRODUCED BY THE DOCUMENT	DOCUMENT
France	1. Preserving data communication for one year by telecommunication operators, internet provider services, and any public body offering access to the Internet, such as Internet cafes. Communicating this data to specialist government agencies. Restraining the covered data to technical data: number of connections to electronic communication services, person's total amount of subscriptions data, localization data of the terminal equipment used, and called numbers. 2. Giving a right to specified intelligence services to consult automated processes for personal data (e.g., the national matriculation file, the national identity cards system, or the management system for foreign nationals in France) upon the authorization of the Minister of Interior and the Minister of Defense.	• Law of Combating Terrorism and on Various Provisions Concerning Security and Borders Controls (2006-64 of 23 January 2006)
	3. Blocking administratively internet websites involved in the glorification of terrorism or the diffusion of calls to jihad – and a judge can put a halt on an online public communication service upon the demand of a public ministry or moral entity when it represents a manifestly illicit disturbance. 4. Requiring internet service providers and web hosts to report illicit terrorist content. 5. Allowing judicial police to access under specific circumstances, from the systems set in police's or gendarmerie's locations, needed data for ongoing investigations, which are stored in different systems on French territory.	• Law Strengthening Provisions on the Fight Against Terrorism (2014-1353 of 13 November 2014)
	6. Designing a legal framework for intelligence services to access data and information, by the use of technical means, for surveillance. It also sets a system of rules to deal with the gathered data that is differentiated according to the technical means used to collect the information (e.g., data collected is destroyed after thirty days for intercepted correspondence and captured talks, five years for data connections, ninety days for sound records, geo-tracking and video images, and no more than six years for encrypted information). 7. Obligating internet service providers to install facilities to analyze automatically data (the so-called 'black box') to monitor and detect any suspect behaviors by the use of an undisclosed method. Providing intelligence services access only to metadata, which is separated from the content by host companies – data intercepted is analyzed for 60 days, beyond which it is either deleted or kept if the terrorist threat is confirmed.	• Law on Intelligence (2015-912 of 24 July 2015)
	8. Allowing intelligence services to legally undertake surveillance abroad: it addresses both the content and data of the communication, but is limited to only situations where communications are transmitted to or received from territories exterior to those of the national territory of France. The Prime Minister, or one of his or her delegates, deliver authorization for such monitoring of communications.	• Law on Surveillance of International Electronic Communications (2015-1556 of 30 November 2015)
	9. Merging intelligence services and creating a unique database for all actors involved in the fight against terrorism.	• Propositions Made by the Commission for Enquiry on the Means Undertaken by the State to Efficiently Fight Terrorism, July 2016
The Netherlands	1. Enabling a specialist team at the National Police to combat online jihadist content; publishing an up to date list of online jihadists; and authorizing law enforcement agencies to sanction Internet companies which (after being warned) facilitate 'listed' terrorist organizations through the spreading of jihadist content. 2. Websites that use hate speech or call for violence or discrimination will be taken down. 3. Establishing a citizens' hotline where concerned citizens can report jihadist (terrorist, hatred inciting and violence-glorifying) content on the internet and social media.	• The Netherlands Comprehensive Action Programme to Combat Jihadism – 2014
	4. Authorizing Intelligence and Security Services (under specific circumstances) to conduct surveillance and within this context to record information, to install observation, registration and tracing instruments, location positioning equipment, to penetrate any security, to introduce technical devices to undo the encryption of data and to copy data stored or processed by automated means, to tap, receive, record and monitor in a directed way any form of conversation, telecommunication or data.	• Intelligence and Security Services Act - 2002

COUNTRY	TOOL/POWERS INTRODUCED BY THE DOCUMENT	DOCUMENT
The Netherlands	5. Authorizing the services (with the aid of a technical device), to receive and record specific and non-specific communication via a wireless connection (non-cable-bound, also called ether communication e.g., mobile telephony and satellite links), along with telecommunications originating from or intended for other countries and to monitor the communication. 6. Enabling the services (under specific circumstances) to turn to providers of public telecommunication networks and public telecommunication services with a request to furnish information related to all the traffic that has taken place or will take place via a public telecommunication network, and such a request is legally required to be fulfilled.	
	7. Authorizing public prosecutor to determine that data obtained through surveillances (by means of a technical device which records signals, the recording of confidential communications, the recording of telecommunications or the requesting of data of a user and the telecommunication traffic data pertaining to that user,) may be used for the purpose of investigations.	• Act amending the Code of Criminal Procedure and certain other laws to regulate powers to demand access to data (Access to Data «General Powers Act») – 2005
	8. Equipping particular law enforcement agencies with special investigative powers such as surveillance, infiltration, pseudo-purchase and wiretapping (these powers can be used only when there is some kind of indication that a terrorist attack is being prepared).	• Investigation and Prosecution of Terrorist Offences (Extension of Powers) Act) – 2007
United Kingdom	1. Defining offences that can provide the basis for prosecuting individuals who have used the Internet to support terrorist activities: a. Providing, receiving or inviting others to receive training, or undertaking self-training, in the making of or use of firearms, radioactive material or related weapons, explosives or chemical, biological or nuclear weapons for terrorist purposes via the use of the Internet. b. Possessing articles which raise a reasonable suspicion or have been proved to be in relation with the commission, preparation and instigation of an act of terrorism. c. Collecting, having or making a record of information (including photography or an electronic record) of a kind likely to be useful for someone to commit or prepare a terrorist act, or to be in possession of any document or containing information of this kind. The document has to be practical for someone and be possessed by an individual without reasonable reasons, which was useful to authorities to intervene in cases where they did not have evidence that the suspect was engaged in activity associated with terrorism. d. Inciting another person to commit terrorist act in or outside the UK (e.g., maintaining websites or chat forum used to publish materials that incite terrorists to murder, such as in Iraq).	• Terrorism Act 2000 • "The Use of the Internet for Terrorist Purposes", UNODC, United Nations, New York, 2012 • Task Force, New York 2012.
	2. Setting a legal framework for regulating surveillance activities undertaken by Government agencies in regards to the interception of communication (e.g., intercepting telephone calls or accessing the contents of e-mails) and communications data (e.g., records related to communications but not the content).	• Regulation of Investigatory Powers Acts 2000 (RIPA) • "The Use of the Internet for Terrorist Purposes", UNODC, United Nations, New York, 2012 • Summary of surveillance powers under the Regulation of Investigatory Powers Act", National Council for Civil Liberties.
	3. Creating offences specifically dealing with Internet-based activity that is likely to encourage or assist in the commission of acts of terrorism: a. Publishing a statement intended to directly or indirectly encourage members of a public to prepare, instigate or commit acts of terrorism – including glorification of terrorist acts. b. Spreading of terrorist publications which support encouraging others to commit or plan a terrorist act.	• Terrorism Act 2006

COUNTRY	TOOL/POWERS INTRODUCED BY THE DOCUMENT	DOCUMENT
United Kingdom	4. Providing the police with the ability to issue a notice against an individual (e.g., a webmaster) associated to terrorist content online (either a statement, an article, or a record). Afterwards the content shall be removed from the view of the public. 5. Reinforcing investigatory powers by making a refusal to obey a notice to provide an encryption key a criminal offence. It must be ensured that the suspect does not hide part of the data by utilizing multiple keys that protect different data sets (e.g., to encrypt a hard drive in such a way that there could be two passwords created, one for accessing clean data and the other for the incriminating data). Therefore, the examination of the given material has to take into consideration whether there is any "missing volume" of data.	• "The Use of the Internet for Terrorist Purposes", UNODC, United Nations, New York, 2012
	6. Requiring companies providing communication services to mandatorily retain data for the purpose of investigating and preventing crimes, set out according to a clarified and strengthened legislative framework. 7. Limiting public authorities which might have access to content of extra-territorial content of communications. Intelligence services will continue to require an interception warrant issued by the Secretary of State. 8. Ensuring that the definition of 'telecommunication service' covers internet-based services, and requiring additional regular reporting from the Interception of Communications Commissioner.	• Data Retention and Investigatory Powers Act 2014
	9. Strengthening the legal powers and capabilities of police and intelligence agencies to respond to the increased threats coming from Syria and Iraq as well as prevent individuals from being radicalized in the first instance. 10. Amending the Data Retention and Investigatory Powers Act 2014 by enhancing law enforcement agencies' ability to investigate terrorism and serious crime: a. The Secretary of State is enabled to require communication service providers to retain additional communications data that will allow relevant authorities to link the unique attributes of a public Internet Protocol address to the person (or device) using it at any given time; b. Communication data is not about the content but rather is related to the data required to identify the sender or recipient of a communication, the time or duration of a communication, the type, method or pattern of a communication, and the telecommunication systems used or the location that the person was communicating from.	• Counter-Terrorism and Security Act 2015
	11. Gathering all powers involved in the acquisition of electronic communications and to put them into a single comprehensive piece of legislation. 12. Enhancing the monitoring of warrants issued by the Secretary of State which need to be approved before coming into force by an independent Judicial Commissioner, with more safeguards being introduced in regards to the acquisition, use and retention of electronic data.	• Draft Investigatory Powers Bill, November 2015
Israel[10]	1. Allowing the security services to issue instructions to a telecommunications licensee with respect to the installation of equipment, performance of a telecommunications service, or ensuring technological compatibility to telecommunications equipment, as well as including the provision of access to equipment as much as necessary to perform the roles of the security services.	• Telecommunications Act (Telephone and Broadcast) – 1982
	2. Enabling particular law enforcement agencies to collect digital evidence on the Internet, in both general criminal and terrorism-related cases. 3. Authorizing investigative authorities to obtain (under judicial permission or in urgent and exceptional cases under administrative permission) to acquire data transferred on communication between computers.	• Computers Act – 1995
	4. Authorizing the Prime Minister to set rules determining categories of data found in databases of a licensee are required for the GSS for performing its roles under this law, and requiring that the licensee must transfer such categories of data to the GSS.	• General Security Service Act – 2002

10 Please note that the author focuses only on the legislations concerning the territory of The State of Israel.

COUNTRY	TOOL/POWERS INTRODUCED BY THE DOCUMENT	DOCUMENT
Israel	5. Allowing the usage of the data found in a database (mentioned in section 4) under a permit which specifies the category of data, and will be limited for a period of 6 months (with the exception that the Head of the GSS may extend this period).	
	6. Allowing the head of the police's investigations and intelligence bureau to obtain non-content data from landline and cellular phone companies, as well as from Internet-access providers. 7. Authorizing the police (senior-level officers) to require a telecom operator to provide the police with an updated file containing: identifying details of all of its subscribers (including unique device identifiers for their phones or parts), information concerning the mapping of its cellular antennas (including identifying details for each antenna and its area of coverage). 8. Establishing an information database of gathered information (which includes: listed and unlisted telephone numbers, names of mobile phone subscribers, serial numbers of mobile phones, and maps of antenna locations). 9. Permitting access to communications data in a case of misdemeanors.	• Criminal Procedure (Enforcement Powers – Communication Data) Law – 2007
	10. Redefining and broadening, among other things, the definitions of terrorist organizations, terrorist infrastructure zones (an extraterritorial area, providing the legal ability for a government to exercise authority beyond its normal boundaries), and terrorist acts. 11. Identifying, as a punishable offence, usage or transfer of property to assist, promote, or fund the perpetration of a terrorist offense or providing compensation to a person who either committed or planned on committing a serious terrorist offense.	• Counterterrorism Act – 2016 (will come into effect on November the 1st 2016)
Poland	1. Authorizing the Head of the Internal Security Agency (ABW) to order classified procedures against any non-citizens who are suspected of activities which may lead to terrorist acts (with the aim to identify, prevent or combat terrorist crime) such as: a. accessing and recording conversations conducted through telecommunication networks. b. accessing and documenting correspondence conducted through electronic communication. c. accessing and documenting data contained on digital data media, end-user tools, and ICT systems. These activities cannot exceed 3 months, with a possibility to extend this duration. 2. In case of a threat or presence of any kind of terrorist event which affects the ICT system of public administration and ICT systems of critical infrastructure, the legislation allows implementing a scale of 4 security alarms. They are a framework on which particular coordinating procedures for ensuring security may be conducted. 3. In aim to detect, prevent and counter terrorist events crucial from the perspective of: – ICT system of public administration entities – ICT networks, included in the list of critical infrastructure systems – ICT systems of owner of critical infrastructure or data transferred in these systems, ABW can conduct so called evaluation of the security. The procedure is based on conducting security tests on ICT system in aim to identify its vulnerabilities. To do so the Agency can produce and access tools and software dedicated to this purpose. By using them the Agency can access partially of fully ICT systems.	• Counterterrorism Act – 10 June 2016

COUNTRY	TOOL/POWERS INTRODUCED BY THE DOCUMENT	DOCUMENT
Poland	4. In the event of acquiring information about a terrorist activity involving systems and data described in section 3 or in order to prevent and detect terrorist crimes (in this field), the head of ABW can order access to information about the structure and functioning of an ICT system such as a computer password, access codes and other data which allows access to the system. 5. The bill introduces so called denial of access, in other words, possibility for a court to order a blockage of access to particular data included in the ICT system, which is connected to terrorist activity or access to services which served or used to create event of terrorist means. There is a whole procedure that enables to introduce this instrument. 6. The head of the ABW is authorized to document events which breached the security of an ICT system (indicated in the bill), including, among other things, the identification of the source of the breach, a description of the stated event, the methods which were used by the actor or entity which caused the breach, and a description of the damages in the system. On the basis of this information, ABW analyses and creates recommendations which should be implemented by the indicated entities.	

By analyzing selected bills and regulations, it is noticeable that the significant growth of the usage of cyberspace for terrorist activities leads to the introduction of new and more sophisticated counterterrorism mechanisms. There is a need for a public debate about the efficiency of these mechanisms, a discussion about best practices in the implementation process of particular instruments and a plan for future steps. This short brief aims to contribute in this debate.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000. The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.

The Kosciuszko Institute organizes European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.

Office: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: ik@ik.org.pl

More on the European Cybersecurity Forum: http://cybersecforum.eu/

More on the European Cybersecurity Journal: http://cybersecforum.eu/en/about-ecj/