CyberROAD: Developing a Roadmap for Research in Cybercrime and Cyberterrorism

by Peter Kieseberg, Olga E. Segou and Fabio Roli

The CyberROAD project – a collaboration between several major European research institutions, companies and stakeholders - develops a European research roadmap for researching and fighting cybercrime and cyberterrorism.

Cybercrime and cyberterrorism represent a fundamental challenge for future societies, especially given the increasing pervasiveness of interconnected devices, such as home automation systems, connection of industrial systems to the Internet, the Internet of Things and simple commodity items in the area of wearable computing and the storage of private data in the cloud (see Figure 1). Public awareness of cybercrime has increased of late, owing to more frequent reports of online criminal and terrorist activity, as well as the increasing level of damage that can result from successful attacks. The damage caused by such activities in recent years is estimated to be large [1], although the actual figures are a subject of debate - which often becomes political. Current R&D activities in information and communication security do not address the problem at a global level, either in terms of the geographical coverage, or in terms of the involvement of all relevant stakeholders. CyberROAD bridges this gap by drawing together a wide network of expertise and experience, to address cybercrime and cyberterrorism from a broad perspective.

CyberROAD aims to identify the research gaps needed to enhance the security of individuals and society as a whole against forms of crime and terrorism conducted via and within cyberspace. This research addresses current technologies to some extent, but its main challenge is to anticipate tomorrow's world of interconnected living, in particular the dangers and challenges arising from the further incorporation of the digital world into our offline life, building atop initiatives such as [2].

We focus on the following fundamental questions:

- When does crime become cybercrime? When does terrorism become cyberterrorism? This separation is critical in order to identify the research questions that are specific to the cyber-environment, as opposed to the questions still unsolved in common (offline) crime and terrorism.
- How can we subdivide cybercrime and cyberterrorism into meaningful categories? This helps identify subclasses based on common attributes in order to rank the identified research gaps.
- What are the real economic and societal costs of cybercrime and cyberterrorism? As indicated in [2], the costs are often dramatically increased in political discussions. Objective and accurate figures are needed in order to accurately assess the importance of the identified research gaps.
- What are the major research gaps and what are the challenges that must be addressed?
- Once key research gaps have been identified, how do we pinpoint appropriate questions that need to be tackled by research projects? Appropriate approaches to research must be clearly defined.
- How can we test and evaluate security solutions, and to what extent can we test real solutions? Testing is critical in this area, but many challenges exist, especially when it comes to developing test beds for criminal environments and case studies in real life (criminal and terrorist) ecosystems.
- What economic, social, political and technological factors will foster cybercrime and cyber-terrorism? This question focusses largely on the influences of society and the availability of technologies on cyberspace, but also on the influence of cybercrime and cyberterrorism on the development, and especially suppression, of new technologies, which in turn lead to changes in society (see Figure 2) [3, pp. 15].

The main outcome of CyberROAD will be a research roadmap regarding the analysis and mitigation of cybercrime and cyberterrorism. This roadmap will be developed based on a gap analysis regarding future scenarios extrapolated

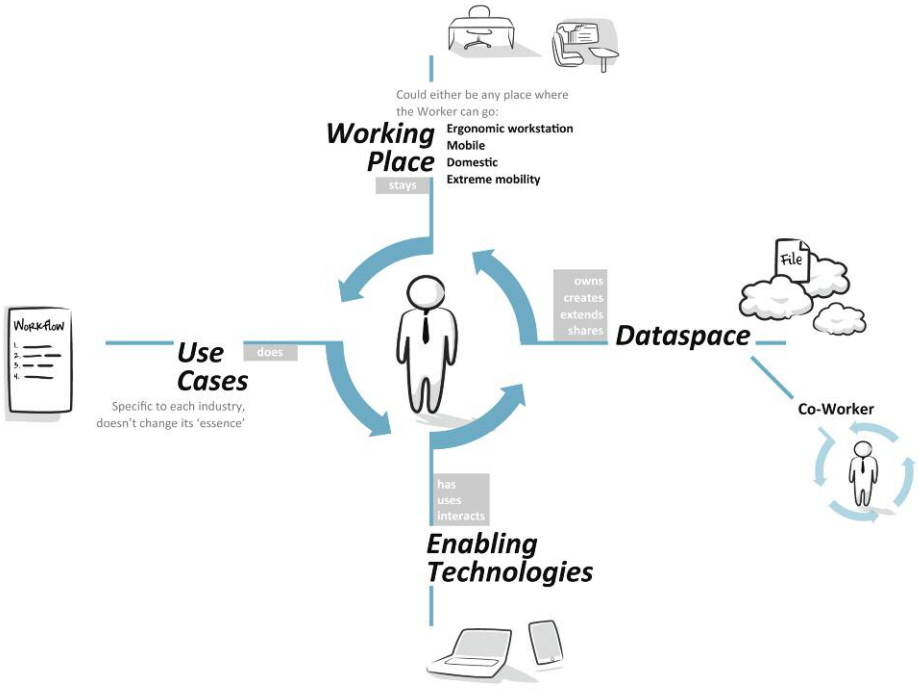

Figure 1: The integration of ICT into everyday life (by courtesy of Enrico Frumento, CEFRIEL • ICT Institute Politecnico di Milano)

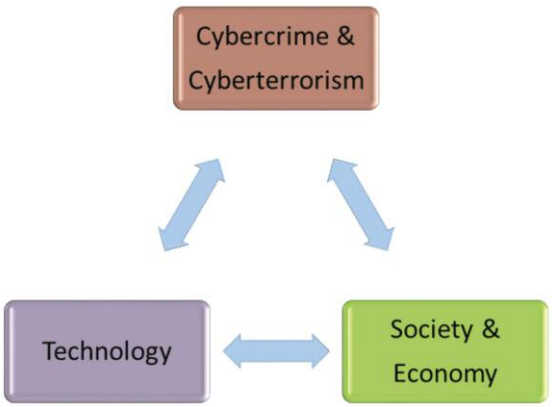

Figure 2: Technology, Society and Cybercrime/Cyberterrorism

from the current state of technology and society, compared to the means of defence (legally) available to system owners and society as a whole. This includes conducting risk assessments for future and emerging technologies with respect to their impact in order to rank the importance of the identified research roadmap topics. While the main driver for the roadmap is the continuing penetration of society by new technology, the topics of ethics, privacy, law, society and fundamental rights are inextricably linked to this area and, as such, research questions relating to these issues are tightly incorporated into the project.

The identified roadmap items will serve as starting points for the development and setup of new projects, largely on a European level. CyberROAD will also serve as an incubator for enhancing the state of research regarding cybercrime, cyberterrorism and the underlying technological and societal variables.

The CyberROAD project has been running since June 2014 and is funded by the European Commission through the seventh framework programme. The project is led by the University of Cagliari and carried out by a team of 20 partners across Europe, ranging from (governmental) stakeholders to universities and private industrial partners.

Links:
http://www.cyberroad-project.eu/
The survey homepage: http://cyberroad.eu/

References
[1] R. Anderson, et al.: "Measuring the cost of cybercrime", The economics of information security and privacy"pp. 265-300, Springer, 2013.
[1] C. Wilson: "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress", Library of Congress Washington DC congressional Research Service, 2008.
[2] J. Larosa, et. al. (2014). ERCIM White paper on Cybersecurity and privacy research, http://www.ercim.eu/images/stories/pub/white-paper-STM.pdf
[3] M. Yar, "Cybercrime and society", Sage, 2013.

Please contact:
Peter Kieseberg, SBA Research, Austria
E-mail: pkieseberg@sba-research.org

Exciting News from IFIP TC6: Open Publication is here!

by Harry Rudin

The IFIP (International Federation for Information Processing) Technical Committee 6 (TC6) held its spring 2015 meeting in Toulouse just before its 2015 Networking conference. At the meeting, the TC6 Chairman, Aiko Pras, announced continued progress with the TC6 open digital library: http://dl.ifip.org/. It is now truly operational.

TC6 deals with Communication Systems and organizes a number of conferences each year, one of them being "Networking". What is exciting is that the papers from the conference are freely available online: Have a look at http://dl.ifip.org/db/conf/networking/networking2015/index.html

Freely available means that no fee is charged for access: One needs neither to be a subscriber nor to pay a per paper access fee. It is also worth pointing out that the authors did not have to pay to have their papers published either.

At many TC6 conferences a best paper award is given. For the 2015 conference, out of the over 200 papers submitted, 48 papers were selected for presentation. The winner of the best paper award is "Information Resilience through User-Assisted Caching in Disruptive Content-Centric Networks" by Vasilis Sourlas, Leandros Tassiulas, Ioannis Psaras, and George Pavlou. Interested? Then just have a look at http://dl.ifip.org/db/conf/networking/networking2015/1570063627.pdf

The plans are to make open publishing available for all IFIP TC6 conferences. In the meantime, enjoy the papers already available!

Link:
http://dl.ifip.org/

Please contact:
Harry Rudin
Swiss Representative to IFIP TC6
E-mail: hrudin@sunrise.ch