Shaping the Future of Transatlantic Civil Security Education

Jadranka Denkova

Goce Delcev University, Stip, Republic of Macedonia

Security Europe consist of online access for policy developments analysis, tenders contract awards, conference event calendar, information hotline. Other services provided monitoring reports by sector, customized surveys of technology potential, security workshops – EU project, funding and training. For civil security in EU trends is current developments, it means huge push toward collective land/sea surveillance of EU external borders. Naval picture will link to civilian sitcom /sat-radar to costal radar stations. Civil public authorities with need to know (police, Intel custom, transport, border guards) will pull info from system. Other things that are essential are raising emphasis on cyber defenses, with operational research budgets to grow at national EU levels. Standardization of security technology to benefit public end-users will get far more emphasis. New home-affairs give initiatives in: confiscation of criminal assets/money, creation of new cyber-crime Centre within Europol, anti-corruption" report cards" at national local levels. Thus: judicial, police and border-guard links are strong – and bound to grow tighter among 27 EU nations of threats grow.

Top civil security threats to EU in descending order: organized crime (financial fraud, goods, counterfeiting, smuggling, illegal, drugs), cyber-attacks in all variants (denial -of-service, biz espionage, critical infrastructure). As well as illegal immigration from externally-driven factors (civil wars, poverty, etc.), terrorism, climate change are civil security threats.

Challenge in investment and national Security is related European governments are cash-strapped, sale of government stakes to raise government revenue but lack of money is not the best motive and do not underestimate the strategic rationale of outside investors. It mean address the challenge across define public and private interests in key infrastructure and industry assets. Set up criteria to determine what kind of investors are acceptable (political and economic perspective), an interagency review process and adopt open communication policy.

Supply chain in Security are concern for produced extended global supply chains and thus increased dependence and vulnerability, product counterfeit increasing, so is espionage and question what if critical parts of the national critical infrastructure fail and/or are manipulated. Challenge for supply is related in raise awareness across all critical

infrastructure sectors. As well engage business to help identify dependence on critical components and lunch public - private initiative to engage in supply chain- related information exchange are main factor for strengthening security. Make supply chain risk management part of public and private acquisition.

In this content is necessity to enfaces, influence activities and social media: Beware of manipulation. In this contents challenge is related with social media like Facebook, twitter, mobile etc. We address the challenge if it concentrate towards source validation, use and develop technologies to identify and track Social media manipulation, train and educate users, review communications policy: what type of media is best suited for what messages, track and trace missing citizens with the help of Social Media.

Non-State Actors and technology access to kinetic and non-kinetic capabilities, significant financial leeway of non-state actors and electronic surveillance and interception tools can be used to spy on emergency responders. Actors and technology consider ambivalent nature of technology transfer and how sensitive technologies will be defined in the future (export control), strengthen financial intelligence. Establish monitoring tools and capabilities to track technology flows and identify networks among key actors.

Security-related regulation is a new domain. For that challenge is infrastructure fusion due to ubiquitous use of information and communication technology. Original components not designed to be interconnected in complex networks, existing safety regulation is sector driven, security regulation still underdeveloped, synchronizing technology development and regulation. For that address the challenge in clarify protection goals, order cross-sector assessment of existing regulation, develop continuity requirements for assets that are critical for various sectors, set up dialogue among regulatory agencies, advance incentive-based regulation for safety and security.

Conclusions for Civil Security Education is: strengthen capabilities to anticipate future trends and developments (e.g. scenario, technique, serious, gaming, thinking about ”unknown unknowns”).

Broaden understanding for interplay between national security and corporate security. Advance mutual understanding of public and private risk perception and risk management. Discuss likely (positive and negative) impact of future technologies on civil security.

Forge closer ties between regulatory community and security community.