EEF.GAL/4/18
23 January 2018

ENGLISH only

Organization for Security and Co-operation in Europe

First Preparatory Meeting of the 26th OSCE Economic and Environmental Forum
22-23 January 2018
Vienna, Austria

by **Ms. Rasa Ostrauskaite**
Co-ordinator of Activities to Address Transnational Threats, OSCE

Excellences,
Ladies and gentlemen,
Colleagues,

Allow me to thank the organizers of the First Preparatory Meeting of the 26th OSCE Economic and Environmental Forum for inviting me to address this session on security implications of the digital economy.

The expansion and security of the digital economy has indeed become a very important topic. And it is not difficult to understand why: Currently, the digital economy is estimated at almost three trillion dollars, an impressive accomplishment given that the size of the largest sector – agriculture - is estimated at 3,2 trillion dollars by the World Bank.[1]

Digital technologies have found their place in nearly every part of the economy and created new opportunities and potential benefits – enhancing productivity, income and social well-being, creating new jobs and increasing employment in some existing sectors.

With a projected 1.1 billion new Internet users in 2020**,** the digital economy is set to grow, benefitting on the way from new technological developments and more economies opening up to the online market.

However, while the digital economy has great potential, it also brings about new challenges and threats. New attack vectors focusing on digital disruption created new means by which whole industry sectors can be compromised. This, in turn, can have a serious impact on national and international security.

For instance, as financial institutions become more data-driven digital businesses and more financial services are delivered online, cyber risks are increasing. If these cyber risks and responses are not well managed, they could threaten the stability of the entire financial system, and, more importantly, the livelihoods of millions of citizens. This is not just a concern for businesses but States too.

Looking at the issue in broader terms, another concern are attacks against critical information infrastructure and services that enable the digital economy, such as the electricity grid.

[1] Agriculture, value added (current US$) https://data.worldbank.org/indicator/NV.AGR.TOTL.CD

The key message is that the protection of key services and infrastructure enabling the digital economy is fast becoming a principal national security concern, forcing national authorities to re-think who needs to contribute to it.

Central to these deliberations is building up meaningful co-operation with the private sector, both on the national- and international level. This was also an important consideration when the OSCE participating States (pS) adopted the 16 confidence building measures (CBMs) designed to reduce the risks of conflict stemming from the use of Information and Communication Technologies (ICTs).

For instance, through CBM 14, pS committed to promoting public-private partnerships (PPPs), and to develop mechanisms to exchange best practices of common security challenges stemming from the use of ICTs.

Participating States further committed to encouraging responsible reporting of vulnerabilities affecting the security of ICTs, and share information on remedies to such vulnerabilities including with businesses and industries (CBM 16).

What these measures demonstrate is that, even though the CBMs are primarily designed to promote trust between States, this sort of trust cannot be built without the input of the private sector, or indeed enablers of the digital economy.

Unfortunately, as experience shows, developing effective PPPs is not always easy. Contentious issues include, whether to legislate co-operation or to focus on voluntary co-operation; the desirability of private sector involvement in national security; or, sensitivities surrounding the sharing of classified information - to name just a few.

Apart from establishing meaningful PPPs, protecting the digital economy also requires States to heavily invest in technology, infrastructure, co-ordination mechanisms, legislation as well as skills necessary to prevent, detect and investigate pertinent threats.

Closing the skills gap in the public sector appears to be a particular challenge for States. The simple truth is that good expertise is scarce, highly sought after, and often snapped up by the private sector.

With the continuous proliferation of ICTs it is fair to expect that the challenge for the public sector to train, recruit and retain experts will not be solved any time soon.

In fact, a recent Analysis[2] undertaken by the Transnational Threats Department in connection with the implementation of the aforementioned CBMs revealed that 60 % of pS would welcome assistance with developing human resources in the field of cyber/ICT security.

As a result, we intensified efforts related to disseminating good practices on topics such as effective national cyber/ICT security strategies; protecting critical infrastructure from ICT related threats, or national co-operation models between authorities and relevant non-governmental stakeholders.

[2] See Analysis of the Implementation of the Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies (PC.CBM/5/17 of 24 March 2017)

In addition, the Department trains law enforcement and judiciary personnel in IT forensics and digital evidence. For instance, we are currently implementing a two-year long project for criminal justice practitioners in South Eastern Europe related to combating cybercrime and cyber-enabled crime.

Ladies and Gentlemen,

Let me finish by stressing that despite some of the security risks and challenges in securing the digital economy, the benefits by far outweigh the negatives.

Every day billions of online transactions contribute to the prosperity of a very large section of the global population.

Taking this into account, addressing pertinent security concerns should not be seen as a burden, but an investment that allows for emerging economies to benefit from this new way of doing business.

I am particularly happy to see that the OSCE is contributing to this effort, by offering a unique platform to both, harness the benefits of the digital economy as well as discuss related security concerns.