DiPLO
www.diplomacy.edu

OSCE Workshop on Effective Strategies

to Cyber/ICT Security Threats

Lessons Learned

from the Scenario Exercise

DiploFoundation

Belgrade, December 2015

Background

DiploFoundation organised a scenario exercise within the OSCE Chairmanship Event on Effective Strategies to Cyber/ICT Security Threats, on 30 October 2015 in Belgrade, Serbia[1]. The event was part of the formal programme of the Chairmanship Event, and involved over 80 representatives from participating OSCE states and the private and civil sectors based therein. The exercise included a simulation where participants explored, reviewed, and discussed communication lines which could be taken into consideration when responding to a cyber-incident.

The simulation exercise encouraged open discussion among delegates, divided into small groups, about the stakeholders that are or should be involved in handling a cyber-incident (including diplomats as well as representatives from the public sector, private sector, and civil society), and the procedures that exist or should exist on a national, regional, and international level, to reduce the risks of misperception, and of the possible emergence of tension or conflict due to cyber-incidents. The discussions were guided by expert group facilitators who took notes and contributed to preparing these lessons learned.

Lessons learned were compiled as a summary of inputs from group discussions, aiming to reflect on the competences and roles of various stakeholders, and suggest desired patterns of communication among them. The document follows the outline of the exercise which was based on imaginary cyber-incident scenarios[2] in countries without functional emergency response mechanisms: it first looks into how to react to an incident and de-escalate the situation; then, it takes the lessons and suggests approaches to increase readiness to respond to incidents and prevent unnecessary political escalation.

Lessons learned present only the observations of the exercise and group discussions by DiploFoundation facilitators. They are, however, not a formal position of DiploFoundation, the OSCE, or any of the expert facilitators or event participants. The document should serve as basis for further discussions, especially in the context of understanding the practical aspects of OSCE Confidence Building Measures (contained in PC.DEC/1106[3]).

[1] Details available at: http://www.diplomacy.edu/calendar/simulation-exercise-during-osce-chairmanship-event-belgrade
[2] Video available at: https://www.youtube.com/watch?v=_BtebHloMqM&feature=youtu.be
[3] Documents available at: http://www.osce.org/pc/109168

Lessons learned: Response to an incident

Emergency response mechanism

Urgent emergency response measures need to be undertaken to stop the attacks. If the country has a national CERT and other CERTs, the national CERT should coordinate the efforts. If there is no (functional) national CERT, a task force should be established to review the situation and undertake necessary measures. Since stopping the attack involves technical knowledge, the task force should be composed mainly of IT and cybersecurity experts: it is advised to look for experts available within government institutions, telecom regulatory authorities, and experts from local Internet service providers (ISPs), telecom providers, academic institutions, and other CERTs in the country if those exist. Big IT and security solutions providers (such as Microsoft, CISCO, or Kaspersky) should be invited to assist with their expertise, if needed, especially if those companies have a strong presence in the country (this may cut the time of involvement of experts).

Cooperation

The institution or body in charge of the emergency response to the current incident (a CERT, a task force, or other) should analyse the problem and act through cooperation with major national institutions and IT providers, while collecting and preserving possible evidence in cooperation with the law enforcement agencies (LEA) and the Privacy Commissioner (if these offices exist). Unofficial contact with police and prosecutor contact points should exist at all times, if possible. Constant contact with security sector should also exist, especially in the case of major incidents.

CERTs of other countries should be invited to assist, if needed, either through other CERTs in the country, if those exist (since such connections are already operational), or through professional networks of the academic and technical communities or the IT industry (these can be established relatively quickly since there are no protocols), or through diplomatic bilateral relations with other countries that have strong CERTs – especially in the region (though this may take time).

A single contact point should be appointed to be in constant touch with the media, giving accurate information, as appropriate, in order to prevent panic.

Criminal investigation

The institution or body in charge should report the crime to the LEA, and a prosecutor will need to decide whether to open an investigation, and inform the police of a possible crime. The police should work with the institution in charge to preserve the evidence collected and conduct additional e-forensics, as appropriate, in cooperation with the private sector and other involved institutions.

If the investigation shows the attacks came from another country, LEA institutions should demand that evidence in the foreign country be frozen or preserved. This demand should be made through informal cooperation or through mutual legal assistance treaties (MLAT) – if existing and necessary – with the assistance of the Department/Ministry of Foreign Affairs. International organisations (Interpol, Europol), or regional ones such as Selec should be informed as well.

Political steps

Possible political and diplomatic activity might follow after the emergency response and investigation are underway, and sufficient reliable evidence that explains the situation clearly has been collected and interpreted by the experts (from the CERT or other body in charge of the emergency response), representatives of the LEA, and the security sector. In such cases, diplomats might refer to some of the existing international or regional legal mechanisms and platforms (e.g. the OSCE, the Council of Europe Convention on Cybercrime, UN Group of Governmental Experts reports, or other) or follow up through bilateral relations.

Lessons learned: Increasing readiness

Emergency response mechanism

A country should form a national CERT (and a government CERT) built on expertise and trust with partners.[4] The national CERT should serve as a central hub and contact point of national structures with regard to cyber-incidents.

The CERT should recruit IT experts from the technical, academic, and IT industry sectors. The national CERT should deal with cybersecurity risk management and mitigation plans, conduct risks analysis and gap analysis, and develop situational awareness. It may help to improve procedures and standards for cybersecurity and cooperation on corporate and institutional levels. The national CERT should also establish regular communication with the media.

Exercises and drills should be conducted regularly, involving CERTs, the security sector, and critical sectors at least, with broader participation on some occasions (media, corporate sector, civil society organisations). Trust between these various parties in country, and internationally, should be promoted, in order to achieve an efficient emergency response.

Internal communication and cooperation

Cooperation and information sharing among national bodies need to be facilitated. Communication patterns among institutions should be clear and well organised, encompassing all levels – from experts to highest officials. A government multistakeholder advisory body may be formed, involving major government institutions, critical infrastructure operators, the corporate sector and IT industry, academia and R&D departments, and expert NGOs. Such a body would look into technical and security data and expert analyses, and prepare strategic suggestions, thus translating the technical parameters into political language for high officials. The national CERT should serve as the main communication hub for information sharing and cooperation with regard to cyber-incidents.

Clear communication patterns should be set among institutions and stakeholders – among LEA institutions, various CERTs, various government and security sector institutions, as well as diplomats with CERTs and expert communities. Of particular importance for better understanding and evidence-based decisions, which would prevent unnecessary political escalation of cyber-incidents, is the enhanced and institutionalised communication between the technical community and public authorities, and between diplomats and key national bodies in charge of cybersecurity.

Security sector institutions should create and nurture internal (national) formal and informal communication channels. Communication with the private sector, which is crucial for critical (information) infrastructure protection, should exist through partner relations which ensures two-way information and assistance flow (the private sector has more technical capacities, but the security sector has legal prerogatives) and is much more effective than merely relying on legal reporting requirements that ensure only the bare minimum of communication. In addition, the international nature of business leads to the accumulation of international contacts within the private sector, which can be used to de-escalate conflicts and build confidence. Public-private partnership was agreed to be a good model for information sharing among these two sectors. NGOs and academia were also stressed as potential valuable allies for security sector institutions for both increasing technical capacity and informal networks of contacts and information sharing. Transparency is of crucial importance: in the case of a crisis, but also beyond, it is important that security sector institutions contribute to the government's efforts in a timely fashion, transparently informing citizens of what is going on.

[4] For best practices on CERT, consult BPF 2014 - Outcome Document - Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security from the UN Internet Governance Forum, available at http://www.intgovforum.org/cms/documents/establishing-and-supporting-computer-emergency-response-teams-certs-for-internet-security.

Legal and strategic framework

Good governance in the security sector is expected. It is important to have laws, strategies, procedures (internal communication, decision making, etc.) in place at a national level, in order to ensure a secure cyber-space. Security sector reform, as a method of achieving effective and accountable security sector institutions, is relevant for cybersecurity as well.

Cybersecurity strategy was pointed out as useful framework for the cooperation of various sectors and institutions in the area of cybersecurity. A strategy could set up the cooperation framework; identify key risks, actors, and roles; outline principles and strategic pillars; and define action plans and responsibilities. In order to preserve both a secure and an open Internet, the strategy should bring strong links to human rights.

A strategy should assist the improvement of the legal system, including encouraging the development of legal norms that follow existing international instruments. A law on cybersecurity should be carefully prepared, to formalise roles and responsibilities.

Capacity building, education, and awareness

Awareness of high officials and institutional capacity for cybersecurity should be strengthened. A possible multistakeholder advisory body could help with raising awareness among high-level officials about the situation, risks, and measures in cyberspace.

Capacities, resources, and the efficiency of prosecutors, police, and judges with regard to cyber issues should be increased. Diplomats should be prepared (also through programmes within diplomatic academies) to better understand cyber-issues and be able to use the existing international mechanisms – but also to contribute to building and shaping new regional and global mechanisms and cooperation platforms (including strengthening the OSCE work). Capacities for digital policies of public authorities and decision-makers, as well as of the corporate sector and civil society, should be strengthened in order to enhance cooperation and dialogue on maintaining an open and secure cyber-space. Not least, efforts should be invested to raise capacities and awareness of media to follow cyber-issues properly. A national capacity building agency may be formed, which may channel and use existing capacities and offers of non-government training organisations, academia, and the private sector. Capacity-building programmes should run on regular basis.

Cybersecurity competences – technical but also legal, management, and policy knowledge – of critical sectors should be strengthened, by increasing skilled labour though public-private partnership programmes involving national and local authorities, the private sector, the security sector, and the academic and technical communities. These efforts should be coupled with greater investment in conducting academic and policy research related to cybersecurity and digital policies.

All stakeholders should work towards building a cybersecurity culture in their respective societies, thus making educational and awareness initiatives on all levels of the highest importance. These initiatives must be effective and sustainable in order to be able to deliver the long-term impact needed. On a formal level, cybersecurity should be also introduced to educational curricula in schools.

International cooperation

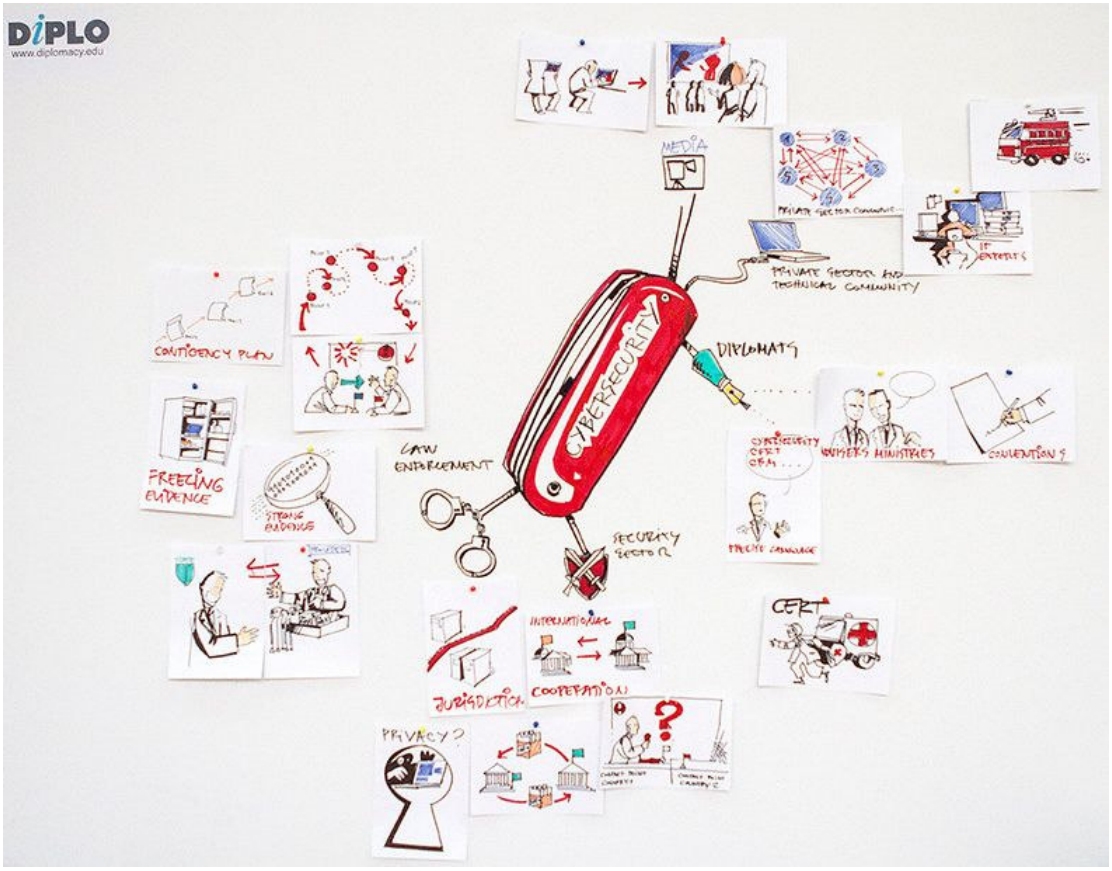
Countries should enhance mutual sharing of information about cyber-risks, strategic and policy measures, programmes, and public-private partnerships. While specific sectors already share information with foreign counterparties – especially the CERTs and technical communities, academia and civil society, and the private sector, all of whom often nurture the emerging concept of open access and sharing – there is a lack of a coordinated approach to sharing critical information at state levels. Greater cooperation of diplomats with these sectors might be needed in order to enable a more structured and coordinated international cooperation in cyber-space.

Formal and informal contacts, confidence building measures (CBM), and information exchange platforms can help build confidence and thus contribute to crisis mitigation and conflict de-escalation. However, due to the specific legal limitations imposed by the need for classified data protection, military and intelligence services should be encouraged to have informal contacts, but to exchange operational information only through formal procedures.

Diplomats should engage more with the cyber-diplomacy agenda in order to strengthen the international legal and cooperation framework and establish greater understanding and cooperation among states with regard to cyber-challenges. This, combined with the greater cooperation of diplomats with other sectors for a coordinated approach, would contribute to building sustainable trust and confidence among countries.

Cybersecurity multi-tool

The main keywords and concepts expressed during the discussions were also visualised on the drawing board throughout the session in form of a cybersecurity multi-tool chart, sketched and updated by Diplo's Creative Lab illustrator Vladimir Veljasevic, and presented as a visual output of the exercise.



Final version of the cybersecurity multi tool chart (a full-size image is available at: https://diplo.smugmug.com/Events/2015/OSCE-Cybersecurity-Meeting/i-qFC7DhJ)