CHALLENGES TO STRATEGIC DECISION-MAKING IN CYBER SECURITY

Authors: Lauri Almann, Kari-Pekka Rannikko, and Lucie Kadlecová, CybExer Technologies

The month of October is recognized as European Cyber Security Month, sparking events on this topic across Europe each year. Prague Security Studies Institute's Cyber Security Academy (CSA) is one such events, offering a forward-looking perspective through its list of distinguished speakers from the Czech Republic and abroad. Its participants represent a cross-section of society, but all aspire to become future leaders with awareness of the importance of cyber security knowledge. Estonian cyber security company CybExer Technologies delivered this year's CSA concluding strategic table-top exercise and provided over 20 students and young professionals with a unique opportunity to test their theoretical knowledge in practice and recognize the most pressing issues for 21st century strategic decision-making in cyberspace.

The following four most prevalent, interdependent cyberspace challenges were particularly emphasized during the strategic exercise:

UNPREDICTABILITY OF A SITUATION

The scenario used in this exercise developed from a seemingly innocent business decision through an election crisis to a life-endangering situation within just a few days. This was made even more alarming as the presented scenario was inspired by real events from the past. This realistic scenario illustrated how cyber threats do not follow any patterns or respect any physical borders, which leads to serious unpredictability of situations in cyberspace.

DEFINITION OF A SITUATION

Determining the severity of a situation unlocks the use of tools and resources necessary to resolve a crisis. However, there are often major differences in opinion among decision-makers concerning how to define the situation, which is a problem closely related to scarcity of data and situational awareness. Quality and accuracy of information determine our decisions. Accordingly, we are faced with the challenge of cautiously navigating a continuous flow of data, especially in the modern era of hybrid threats and disinformation. Furthermore, even if the facts are known, it does not guarantee consensus with regard to the most effective response. It is not uncommon that one group of decision-makers considers a certain situation to be "business as usual" while another group with the same set of information calls it "an armed attack". This is caused by the lack of routine and practiced policies. This is a serious problem because if a decision on the severity of a situation cannot be reached, decision-makers lose valuable time and block the use of appropriate resources.

SHARED SITUATIONAL AWARENESS

The absence of shared situational awareness is another challenge commonly present in practice and recognized through the strategic exercise. Even if all stakeholders are familiar with a set of reliable data, it does not guarantee that they have the same understanding of it. It is, therefore, key to know how to work with the information as well as understand other actors' perspectives and orientation, which, inevitably, involves the willingness to publish or share information and to cooperate with other stakeholders. The actor must have clear guidance on cooperation with domestic authorities, and the public and private sector, but also foreign entities such as those from non-NATO countries.

MULTIDISCIPLINARY APPROACH TO CYBER SECURITY

Finally, the exercise's participants had the opportunity to experience one of the most rapidly-growing challenges to cyber security – the need for a multidisciplinary approach. The general public mistakenly perceives cyber security as an exclusively technical issue. However, modern decision-makers should realize that a multidisciplinary approach is indispensable to fully cover the wide spectrum of activities in cyberspace and to make informed decisions. Cyberspace must cease to be perceived as a purely technical domain, making way for other disciplines such as international relations, international law, diplomacy and strategic communication.

To give a concrete example of a threat vector which touches upon all the challenges introduced above, exercise participants were presented with a ransomware dilemma. Ransomware is the most serious cyber threat vector, which is not only a risk for the future but, in fact, today's reality. The recent case of hacked psychotherapy records in Finland is just one of many examples. The Finnish major ransomware incident illustrates the severity of this type of attack which usually does not concern only technical data breach, but involves much bigger social and psychological issue that has an impact on the whole community.

Given the various dimensions which need to be considered when dealing with ransomware, it is often a provocative topic in strategic decision-making exercises like the one run during PSSI's CSA. The participants are divided into groups that represent public and private institutions. Their organizations are infected with ransomware. The following inevitable and highly uncomfortable question is asked: "Will you pay?" The groups have to consider the ethical, communication and cooperation dilemmas. There is a pattern with regard to the responses of the different groups.

Government entities usually take an extremely stringent moral stand and refuse to pay because "governments do not negotiate with criminals". The private sector is often split, with half arguing to pay the ransom. In addition, the private sector is rarely willing to share information about the attacks and payment of ransomware with their governments. In the exercise, as a result of its "moralizing" strategy, the government loses potentially valuable information, intelligence, and situational awareness. It is then poorly equipped to fight back against this highly dangerous and unpredictable type of cyber attack. The question raised then is whether our current approach to the ransomware dilemma is the right one and whether deeper focus on the four challenges of cyber security introduced above might be a better way forward. Without doubt, uncertainties in the operating environment are increasing and simultaneously causing greater difficulties for decision-making.