THE NEED FOR ANALYTICAL SUPERHEROES

Addressing the nontechnical aspects of cyber threats

By **Ondřej Rojčík**
Head of Strategic Information and Analysis,
Czech National Cyber and Information Security Agency

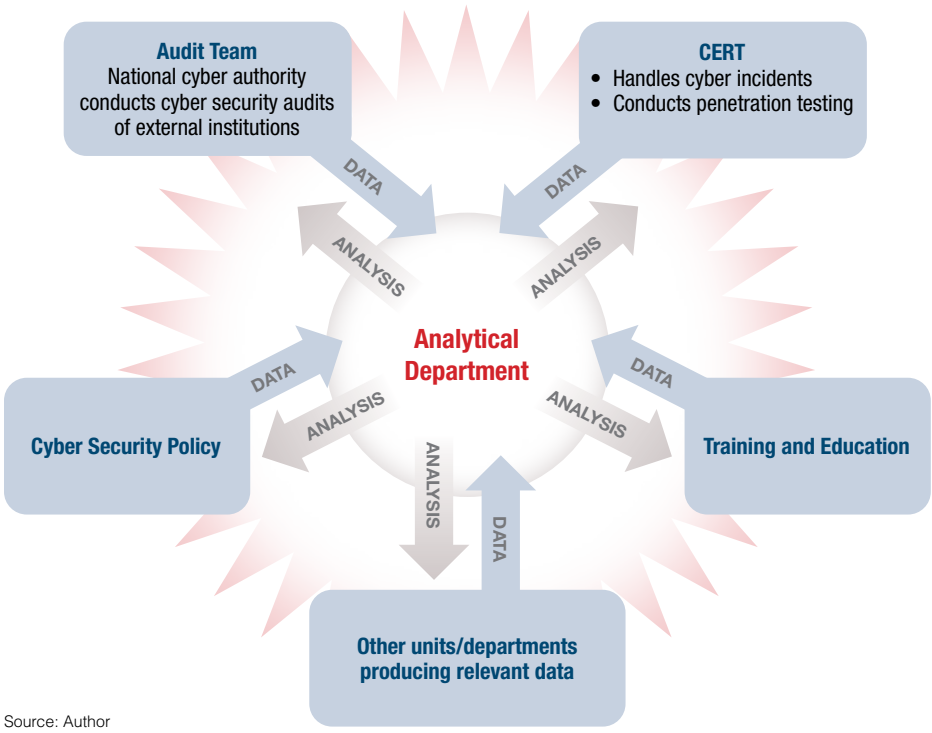
We tend to perceive cyber security as a purely technical issue. Dozens of reports from recent years point out the scarcity of cyber security experts and link this to a general lack of specialists educated in information technology. Emphasizing the relative dearth of technical talent, however, is a rather narrow perspective that doesn't account for the need for many other types of experts with backgrounds and educations that are not purely technical. For example, the labor market is seeking cyber security managers, auditors, lawyers, homeland and international security experts, regional experts, educators and analysts. Nontechnical analysts are responsible for the contextualization of cyber security incidents and trends, a function the Czech National Cyber and Information Security Agency (NÚKIB) has used in many key activities over the past four years. What skills do we need to build capability for nontechnical cyber security analysis?

Contextualization

In December 2018, NÚKIB issued a warning against using technology from the Chinese telecommunications companies Huawei and ZTE. NÚKIB reasoned that use of these companies' products constitutes a security threat because Chinese law requires Chinese citizens and companies to cooperate with state governmental agencies, including the intelligence services. As a result of the warning, system administrators of critically important systems in the Czech Republic have a legal obligation to acknowledge the threat and adopt adequate measures.

NÚKIB is also the key proponent of the Prague Proposals, a cyber security framework that emanated from the 2019 conference on 5G security in Prague. A main point of the Prague Proposals is that in addition to the technical nature of cyber threats, specific political, economic and other behavior of malicious actors should be considered when assessing the security of information technology. Cyber security has political dimensions. In the Czech Republic, experience with analysis of the nontechnical/contextual aspects of cyber security has created a strong bias toward this inclusive approach to cyber security.

The situation of Huawei and ZTE technologies and the Prague Proposals were not the first instances when NÚKIB learned of the need to develop nontechnical analytical



Source: Author

capabilities to address cyber security-related issues. Since 2015, the agency has been executing tabletop exercises for decision-makers, mainly from the government sector. One of the critical lessons learned from these exercises is that with technical data from incidents alone, without broader context, it is almost impossible for decision-makers to identify and take appropriate responses and courses of action.

In-House Analytical Capabilities

To provide contextual information and analyze the circumstances regarding a particular attack, and the legal, political and economic environment of certain actors, appropriate data must be gathered, and sophisticated analytical processes and skills must be developed. It would be very impractical to rely on external partners such as intelligence services or private companies. Intelligence services wouldn't have flexibility in two respects: First, they would rarely have the right information when it is needed. Second, most of the information would be classified, which creates difficulties in terms of immediate usability. As for private companies, it is difficult for a government organization to trust and rely exclusively on a private party and take measures based on their information. However, information from some private vendors can provide a reasonable portion of the overall data mix at a later stage of the analytical process.

NÚKIB has been building nontechnical cyber security analytical capabilities for over four years. The main function is to support NÚKIB's policy cycle and to provide analysis of cyber security issues to top decision-makers in the government and other strategic institutions. Indeed, NÚKIB is the Czech national authority in the field of cyber security. Among other activities, it is responsible for the policy and regulatory aspects of cyber security. To produce appropriate policies and regulations that reflect current issues and developments, there must be a constant state of awareness and horizon-scanning must be conducted daily. Any government institution with nationwide responsibilities in the area of cyber security would benefit from a similar capability.

NÚKIB benefits from having the technical and policy/regulation aspects of cyber security residing under a single roof. This is an effective arrangement, but for organizational or historical reasons, may not be appropriate in many countries. In many national cyber security ecosystems, these two parts of cyber security are separated, if present at all. There can be an independent national cyber emergency response team (CERT), for example, while the policy branch is under the Ministry of the Interior, Ministry of Industry, etc. If the policy branch establishes a cyber security unit within one of these ministries, it would tend to focus on strategic trends only. If it is organized by the technical branch — CERT — the natural tendency could be to stress only the contextualization of technical incidents.

In any type of arrangement, the analytical unit should not be separated from the rest of the organization. The analytical endeavor needs to spread through the organization and throughout the infrastructure (i.e., data and analytical software), including personnel. Specific units that produce relevant data should share that data with analysts who are then able to link it with data from other parts of the organization and with the broader context of external trends. Data interconnection from various parts of the organization is essential. If the data is not pooled, knowledge is contained and isolated in separate parts of the organization. As a result, the value of the data is substantially lower and the analyses inadequate.

Consider it a Project

Any organization interested in establishing a dedicated analytical unit to assess the nontechnical aspects of cyber threats must consider a plethora of factors. These include the highly specific skills of the analysts. However, these fundamental conditions should be met before any workforce development can take place.

Establishing a nontechnical analytical unit should be approached as a project. To successfully run such a project, it is indispensable to define the goals to be achieved, such as what type of services will be provided and to whom. A crucial aspect of such a project is to find a dedicated sponsor, known in project management jargon as a senior figure.

This champion within the organization has ownership of the project, expects the project to succeed and works to ensure its complete realization. The role of sponsor is not merely an official one. Effective sponsorship is only possible if the sponsor is personally convinced of the project's value and is willing to champion it and support its staff at every formal or informal opportunity, throughout all stages of development.

It is imperative to have a clearly articulated vision of how the analytical unit will be developed to advocate for resources to the organization's senior management. High-quality analytical units are not a cheap endeavor, particularly the cost of analytical software, data collection and storage capabilities, and data acquisition as well as maintenance and other recurring fees. And of course, there are the people. Apart from salaries, there will be expenditures for regular training and education. Any project needs a manager responsible for coordination, but even more importantly, dedicated team members who understand the mission and not only support it, but continuously develop the internal processes and the analytical craft of the unit.

It is imperative to have a clearly articulated vision of how the analytical unit will be developed to advocate for resources to the organization's senior management.

Key Competencies

For an efficient analytical endeavor, two groups of staff should work closely together — analysts and a data team responsible for data collection and maintenance of analytical software. Each requires a specific skill set. Analysts need in-depth knowledge of national and international security issues. In some cases, they need regional expertise accompanied by a significant proficiency in multiple languages. They must understand the fundaments of the technical aspects of cyber security, as well as information security policies and processes. Other crucial elements of the job include proficiency in the craft of intelligence analysis, open-source intelligence (OSINT) tools and techniques, and a working knowledge of analytical software supported by the data team. The two most important roles on a data team are the data engineers, who have expertise in big data infrastructure management, and the data scientists, who have in-depth knowledge of data integration, information science and data visualization tools.

Regarding analytical positions, the current market is unlikely to provide candidates with the complete package of skills, making it necessary to compromise and identify key competencies that can be built upon. The following prerequisites are cornerstones for further professional development: boundless curiosity and enthusiasm for the subject; a willingness to constantly learn; the ability to grasp complex and evolving concepts; the ability to understand the implications of cyber issues in the physical world; excellent written and spoken presentation skills in the national language; fluency in English and in the case of regional experts, a decent knowledge of the regional language. From this base, other skills and knowledge can be added.

HEAD OF ANALYTICAL DEPARTMENT	
Analytical Unit • Regional security experts • Transnational security issues experts	**Data Unit** • Data engineers • Data scientists

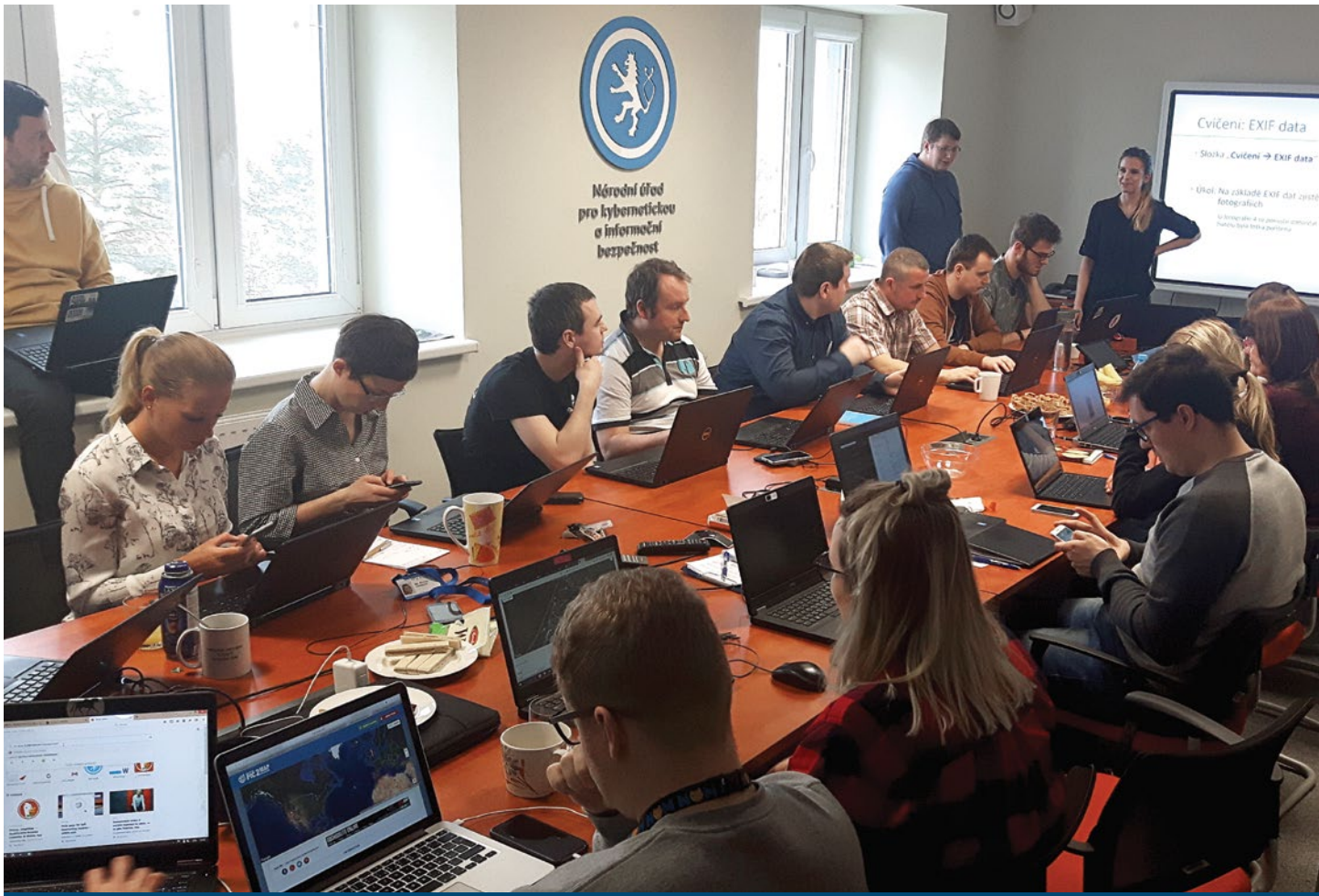
As a relatively small organization, NÚKIB extensively uses on-the-job training, as well as external training provided by institutions such as the NATO School Oberammergau, the NATO Cooperative Cyber Defence Centre of Excellence or private companies. Over the course of approximately three years, analysts undergo training in OSINT, analytical skills, cyber threat intelligence, specialized software and language courses. In that time, all analysts have sufficient opportunity to participate in dozens of analytical projects, support the handling and investigation of critical incidents, and create personal networks for interagency cooperation. After a sufficient period, promotion to senior analyst can be considered.

Professional development in the field of cyber security is never-ending because anything learned in OSINT, cyber threat intelligence, analytical software, etc., more than two or three years ago risks being obsolete. To be up to speed on cyber security, international political development and several other major fields mentioned above requires true analytical superheroes.

After the initial training and general introduction to the job, there is a new challenge: how to motivate the analysts and prevent them from leaving. There is no simple solution, though keeping analysts involved in the major issues of the day and letting them see firsthand the impacts of their work has proved effective at NÚKIB. Another long-term strategy is job rotation in cooperation with the agency's CERT and other horizontal opportunities for professional growth.

Technology Supports the Mission

People are the most critical asset, for which no technology can substitute. Keeping this in mind, the right technology helps to automate as many processes as possible so that analysts can focus on the activities with the highest added value and eliminate any repetitive undertakings. However, there are limits to the absorption of new technologies. Both data and analytical teams can handle only a finite number of software tools and make full beneficial use of them. Therefore, special care must be taken at the beginning of the planning process to choose



Cyber security analysts from the National Cyber and Information Security Agency's (NÚKIB) Strategic Information and Analysis Unit meet at NÚKIB's headquarters in Brno, Czech Republic. NATIONAL CYBER AND INFORMATION SECURITY AGENCY

technology that will best support the mission. It is especially important that the main pieces of analytical software be tools that will help the analysts, not overwhelm them. The data team will consist of people with technical education and data scientists. It is essential that they understand the mission of the unit and the needs of the analysts.

Talent Scouting and Outreach

Since its beginning, the NÚKIB analytical unit has conducted outreach activities to attract new talent to the unit and to the agency in general. Unlike some security agencies, NÚKIB can and must be visible. Outreach activities include lecturing at universities, security or cyber security programs of think tanks and other institutions, and presentations at conferences.

The unit collaborates with the security studies program at Masaryk University in Brno in the Czech Republic, which has generated a substantial pool of applicants for the internship program and jobs at NÚKIB. The internship program has proven to be an excellent introductory opportunity for students interested in careers in government institutions and a great way to practically test potential future co-workers.

Conclusion

Considering international developments and initiatives such as the European Union Toolbox on 5G Cybersecurity or the Prague Proposals, the importance of the nontechnical aspects of cyber security and contextualization of cyber threats will grow in coming years. If national-level institutions responsible for cyber security are to keep pace without depending on third-party expertise, they must establish the necessary analytical capabilities. NÚKIB has been developing this capability for more than four years to support the policy cycle and provide analysis of cyber security issues to top decision-makers in the government and other strategic institutions.

Establishing an analytical unit should be approached as a project requiring long-term dedication from the staff and organizational leadership. The analysts and data team are the most critical assets. Analytical job candidates possessing all the necessary skills are rare. They must be developed by identifying and building on key competencies. Maintaining development in both the technical and nontechnical aspects of cyber security requires true analytical superheroes. □