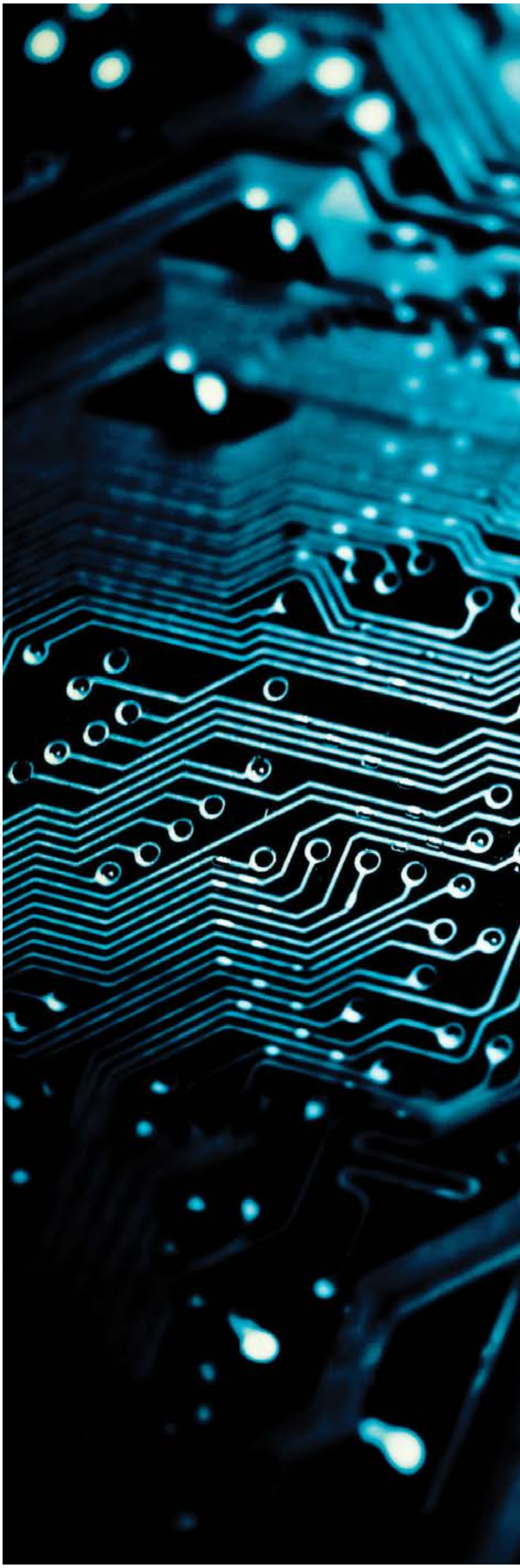
MOLDOVA'S
CYBER SECURITY CENTER

Contacts, trust and communication are key to robust cyber capabilities

By **Natalia Spinu**,
Chief, Moldovan Cyber Security Center,
E.S. Center for Special Telecommunications



Today's cyberspace poses innumerable risks to the security of private companies and public institutions, making them easy targets for cyber attacks by "hacktivist" groups, terrorist organizations or state-sponsored hackers. The days when an organization could withstand that onslaught alone have passed. A collective response based on information sharing can make organizations better prepared and more resilient to these emerging challenges.

Information sharing is voluntary in most cases and is based on a particular need or trust built over time. In some developed countries, legal initiatives have been implemented to encourage and sustain such activities, while reducing risks to the private sector with government as a trusted third party. That is an area where public-private partnerships take place.

In the Republic of Moldova, public-private partnerships don't exist in the cyber domain. Therefore, information sharing typically occurs on an ad hoc basis. This informality severely affects the ability of business and governmental organizations to meet the challenges posed by cyber attacks. Just such a circumstance played a role in recent high-impact incidents in Moldova (CTB-Locker mass infections, Starnet database leak and others).

ISTOCK

Moldovan President Nicolae Timofti passes an honor guard while attending a meeting of the EU's Eastern Partnership in Prague. Moldova's executive branch has led the push to improve the country's cyber security. THE ASSOCIATED PRESS

Many issues hinder information sharing between the private and public sectors and within the public sector alone. They include:

- Uncertainties in national legislation.
- No points of contact between private companies and public institutions.
- Not knowing the structure and responsibilities of the state institutions involved in cyber security, or how and to whom illegal actions or security incidents should be reported.
- Lack of qualified specialists.
- No joint training exercises.

According to current legislation, seven organizations in Moldova are involved in fighting cyber threats and should engage in cyber information sharing at political, technical and civil levels:

- ***Supreme Security Council*** — a consultative body overseeing the execution of governmental policies on national security.
- ***Intelligence and Security Service*** — a specialized organ of state security responsible for combating cyber threats nationwide.
- ***Ministry of Information Technology and Communications*** — department that develops and promotes state policy in the information and communications technology (ICT) domain, including cyberspace.
- ***Office of the Prosecutor General*** — responsible for the coordination and prosecution of cyber crime.

- ***Center for Combating Cyber Crimes*** — a police department specializing in the investigation and arrest of cyber criminals.
- ***National Center for Personal Data Protection*** — an autonomous public authority responsible for the compliance of personal data processing.
- ***Cyber Security Center CERT-GOV-MD*** — a government computer emergency response team.

The Cyber Security Center CERT-GOV-MD is a government-level institution involved in national cyber security development. But that prestige comes with the responsibility to solve complex cyber issues. In recent years, CERT-GOV-MD has performed a number of activities aimed at improving cyber information sharing nationwide. Some noticeable improvements have occurred that can be divided into three areas:

- ***Establishing national and international points of contact.*** In June 2013, CERT-GOV-MD produced an initiative in accordance with an order from the prime minister that requested public administration authorities share information regarding threats and vulnerabilities and report any malicious activity to CERT-GOV-MD. That established an additional pillar in the public-sector information sharing framework and identified contacts at a technical level within government institutions. Another achievement was reached in 2014 when CERT-GOV-MD became an accredited member of Trusted Introducer, an organization that unites European computer emergency response teams. This establishes direct and trusted communication channels within the international cyber security community.
- ***Building trust.*** From 2013 to 2015, CERT-GOV-MD organized a series of international conferences and workshops that brought together representatives from private companies, governmental structures and universities, as well as leading cyber security experts who helped remove the barriers of misunderstanding and cultivated personal relationships.
- ***Fostering communication.*** By engaging simultaneously in the hands-on activities of countering state-targeted cyber incidents, in policy development, and with local, national and international groups and projects, CERT-GOV-MD has developed a unique and holistic understanding of cyber security in Moldova. That allows critical information on the most acute issues to be communicated from the most distant points of government to the highest officials of the country.

Cyber security requires a comprehensive approach. Political will, a nationwide engagement and the involvement of leading experts are key to creating conditions for state institutions to ensure an adequate level of cyber security.

Cyber security requires a comprehensive approach. Political will, a nationwide engagement and the involvement of leading experts are key to creating conditions for state institutions to ensure an adequate level of cyber security. A successful realization of that goal depends on contacts, trust and communication. These are the components that define the role and mission of Cyber Security Center CERT-GOV-MD in Moldova's national cyber information sharing. □