Preface

MELISSA E. HATHAWAY
Chairman of the Council of Experts, Global Cyber Security Center (GCSEC)

The Advanced Research Workshop (ARW) entitled, 'Best Practices in Computer Network Defense (CND): Incident Detection & Response' was held from 11–13 September 2013 in Geneva, Switzerland. It was co-sponsored by the Global Cyber Security Center (GCSEC)[1] and the Geneva Centre for Security Policy (GCSP) [2] to explore common interest issues for improving North Atlantic Treaty Organization (NATO) member states' and partners' cyber defense posture. The workshop was enabled by NATO's Science for Peace and Security (SPS) Program and focused on SPS's key priority areas for cyber defense as well as NATO's cyber defense policy implementation [3].

A multi-disciplinary team of experts from sixteen countries and three international institutions gathered to share experience, knowledge, and positions. Together they generated twenty-one specific findings and twelve papers to help improve the cyber defense posture of NATO member states and their partners.

This report contains actionable information and presents examples that can inform decisions. Of the many findings, five stood apart from the others.

First, no organization should accept the status quo. Our networks are compromised and we have become accustomed to assuming that the adversary has penetrated our defenses. Because of this, many organizations have shifted their security approach toward monitoring and detection. Organizations are monitoring ingress and egress routes, and cataloguing the tactics, techniques, and procedures of their adversaries to understand impact and adversaries alike. New tactics and countermeasures are available to strengthen security postures and become more resistant to cyber threats.

Second, commercial entities are developing, deploying, and operating advanced techniques for network defense. The technologies are accessible and affordable, and they are showing promising results. Techniques range from using moving target architectures to confuse the adversary to turning to the Internet Service Providers and Telecommunications Providers to provide an upstream or forward deployed defense. Other effective techniques include monitoring the dark space of the Internet. Intelligence from upstream dark space monitoring can be used to reprogram deep-packet inspection (DPI) sensors within the enterprise zone to detect zero-day activity.

Third, identifying critical services is more important than identifying critical infrastructures. Services, like electric power, navigation, and telecommunications, transcend national boundaries. Changing the focus from critical infrastructure to critical service may change NATO's approach to protection, resilience, recovery, and restoration of assets. It may also highlight the interdependencies between organizations and nations requiring different approaches to common defense.

Fourth, a baseline assessment enables an organization to identify the current state of the controls it has in place to protect infrastructures, assets, and services. Once a baseline is established, it is possible to prioritize a list of the controls that would have the greatest impact in improving risk posture against real-world threats and then map

progress along the path toward a future state that is more resistant, resilient and recoverable.

Fifth, as we continue to invest in digitizing our infrastructure and everything behind it, security considerations must become a core, non-negotiable component of purchasing and acquisition decisions. Work factor analysis can help acquisition and procurement officials determine whether the vendor's product or service will increase the costs for the adversary.

In a domain where speed is essential, where advanced defense is required against advanced offense, and where collaboration and learning amongst defenders are vital, keeping pace and deploying advanced processes or technology is only possible when you know what is available. Knowing what is possible and available, however, and doing something with that knowledge, are quite different propositions – and the latter is in the hands of the reader.

References

[1] The Global Cyber Security Centre (GCSEC) is a global foundation established in 2010. GCSEC is also known as the 'Centro Internazionale per la Sicurezza Informatica.' The Center is enabled by Poste Italiane S.p.A. with the purpose to carry out and promote study, research, teaching, and training for the benefit of society as a whole and organize projects and events regarding the issue of cyber security.

[2] The Global Centre for Security Policy (GCSP) is an international foundation established in 1995 with over 40 member states for the primary purpose of promoting the building and maintenance of peace, security, and stability through training, research, and dialogue.

[3] The new NATO Policy on Cyber Defense provides a solid foundation from which Allies can take work forward on cyber security. The document clarifies both NATO's priorities and NATO's efforts in cyber defense – including which networks to protect and the way this can be achieved.