Best Practices in Computer Network Defense: Incident Detection and Response
M.E. Hathaway (Ed.)
IOS Press, 2014

Foreword

Malicious cyber activities are an emerging security challenge for all countries, and the members of the North Atlantic Treaty Organization (NATO) share a responsibility to help the global community strengthen its cyber defenses. One of NATO's unique strengths lies in its ability to tap into the operational capabilities and expertise of its members' militaries, and to harness the innovations and technologies of its members' industrial base to ensure national and Euro-Atlantic prosperity, security, and stability. This commitment was reinforced in the Chicago Summit Declaration of May 2012 when NATO members agreed to address cyber threats to improve their common security. [1]

NATO seeks ways to jointly research, develop, implement, and field interoperable cyber defense capabilities to enhance the cyber defense posture of the Alliance. The NATO Communications and Information Agency (NCIA) is instrumental in meeting this challenge. The NCIA is implementing the best of the capabilities used by its member states and transforming the NATO operating model toward being 'services based.' Cyber defense is being consolidated into one portfolio and cyber services will be offered in a catalogue of services from early 2014. This allows NATO to fulfill some of the requirements outlined in the cyber defense policy by broadening the pooling and sharing of more information on defense technologies, intelligence, and best practices.

NATO is also engaging its network of partnerships, which includes one-third of the world's countries, by facilitating cooperation between all stakeholders—public and private, state and non-state, civilian and military—to reduce the vulnerabilities of national critical infrastructures and achieve a minimum level of cyber defense. NATO recognizes that the more alike each country's approach is, the greater protection we all will enjoy.

NATO Science for Peace and Security (SPS) Programme is an excellent mechanism for NATO's members and partners to share effective practices and solutions for emerging security challenges like those presented by malicious cyber threats. The Advanced Research Workshop (ARW) entitled, 'Best Practices in Computer Network Defense (CND): Incident Detection & Response' generated actionable information that will inform NATO cyber defense policy for the foreseeable future. It identified the state-of-the art tools and processes being used for cyber defense and highlighted our technology gaps. It presented industry and government best practices for incident detection and response, and examined indicators and metrics to measure our maturity along that security continuum.

Our security relies on assurances that our defenses—local, global, procedural, political, and technological—are leading edge and address effectively the threats these services face. These defenses are tested routinely, and cannot fail. We believe that this book will provide operators and decision makers with genuine tools and expert advice for computer network defense, incident detection and incident response. It is our hope that the twenty-one findings from the workshop and the technical papers that underpin those insights will serve to strengthen the cyber defenses of the global community.

Mr. Koen Gijsbers
General Manager, NATO Communications and Information Agency
November 2013

References

[1] Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, 2012. *Chicago Summit Declaration*, para. 49. [online] Available at: <http://www.nato.int/cps/en/SID-D03EFAB6-46AC90F8/natolive/official_texts_87593.htm?selectedLocale=en> [Accessed 15 November 2013].