National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DESIGN CHALLENGES FOR INTEGRATING CYBER SECURITY IN NEXT GENERATION NAVAL NETWORKS

LCdr J.E. Rix

JCSP 44	PCEMI 44
Exercise *Solo Flight*	**Exercice *Solo Flight***

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44 – PCEMI 44
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

DESIGN CHALLENGES FOR INTEGRATING CYBER SECURITY IN NEXT GENERATION NAVAL NETWORKS

LCdr J.E. Rix

"This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 3005

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Compte de mots: 3005

DESIGN CHALLENGES FOR INTEGRATING CYBER SECURITY IN NEXT GENERATION NAVAL NETWORKS

Network centric warfare has revolutionized how nations design and build naval platforms for the contemporary operating environment. Advances in the cyber domain have contributed to unprecedented levels of technical interconnectivity amongst multinational Communities of Interest (COIs), but have also introduced new and complex threat vectors to cyber security architectures. Complicating the design challenge for diverging cyber requirements is the need to set multinational interoperability standards for cryptographic systems that protect critical information exchanges. It is in this complex environment that capability developers must navigate as they design the network architectures that will support multinational Command and Control (C2) exchange requirements now and into the future. This paper will demonstrate how the complex problems associated with capability development of maritime networks can be overcome by balancing competing standards for system interconnectivity and cyber security in order to meet the agility demands of modern network centric warfare.

This analysis will include two main areas of focus that have been disrupted in the modern cyber era; traditional cryptographic interoperability and multi-domain networking. First, cryptographic modernization will be examined to demonstrate how capability developers can best manage the competing requirements of cyber security and baseline interoperability in increasingly diverse multinational and technical environments. This discussion will argue that a balanced approach to cryptographic modernization requires adherence to existing standards while also integrating potentially disruptive technologies. Secondly, the degree of interconnectivity between traditional enterprise networks and platform level networks, more commonly referred to as Supervisory Control and Data Acquisition (SCADA) networks and Combat Management Systems (CMS) will be examined. This analysis will be conducted to demonstrate how interconnectivity requirements between two different network families have proliferated but only at the expense of increased risk to cyber security at the platform level. It will argue that traditional risk adverse concepts of network isolation from the foundational Bell-LaPadula Model for access control[1] and the Clark Wilson Model for system integrity[2] have been overtaken by modern cross domain solutions that support higher risk tolerances in achieving a balance between security and operational functionality.

A BALANCED APPROACH TO CRYPTOGRAPHIC MODERNIZATION

The standardization of cryptographic material is one of the most complex interoperability challenges faced by multinational coalitions supporting modern network operations.[3] It also remains one of the most important factors in cyber security for supporting confidentiality, data integrity, entity authentication and data origin authentication in military systems.[4] Striking a balance between what is needed to maintain interoperability and what is required from a cyber security perspective is the challenge of modern capability developers working in this domain.

In examining these opposing objectives more closely, it is necessary to understand the role of cryptography in modern fortress security architectures. Simply put, fortress security

[1] Len LaPadula, Elliott Bell, “Secure Computer Systems: Mathematical Foundations,” *MITRE Technical Report 2547, Volume I* (March 1973): 12.

[2] David Clark, David Wilson, “A Comparison of Commercial and Military Computer Security Policies,” *MIT Laboratory for Computer Sciences IEEE* (16 June 1987): 189.

[3] US Office of the Chief of Naval Operations, “AUSCANNZUKUS MIW Experimentation Report 2017,” (Washington: Office of the Chief of Naval Operations, 2018), 27.

[4] Alfred Menezes, *Handbook of Applied Cryptography* (Boca Raton : CRC Press, 1997), 4.

architectures represent the current baseline for military grade cryptographic solutions. These architectures are distributed in nature, are centrally managed, and have highly regulated access controls. From a cryptographic perspective, fortress security is highly reliant upon perimeter defences that restrict access and control exchanges across network boundaries.[5] It is for this reason that principles of fortress security have been and remain the gold standard in military cryptographic systems for older Suite A, and newer Suite B cryptographic requirements.[6] That said fortress security is reliant upon common computing environments and cryptographic architectures that are complex in nature and difficult to manage in a multinational environment.

In the defence sector, the generation of standards that support common cryptographic foundations are managed through multinational interoperability forums. The Combined Communications and Electronics Board (CCEB) is a Five Eyes organization that has continuously supported technical interoperability since its inception in 1942 and is still functioning as one of the premiere multinational standards forums for allied military systems interoperability. In the maritime environment, Five Eyes interoperability standards are managed by the AUSCANNZUKUS Maritime Information Warfare (MIW) organization.[7] These forums interact with the NATO Standardization Office (NSO) through the NATO Consultation, Command and Control Board (C3B) to support the convergence of both Five Eyes and NATO technical interoperability standards for Command and Control Information Systems (C2IS) including cryptographic systems.[8] The cryptographic objective of these interoperability boards is

[5] Jenny Watson, *Maximum Security* (Indianapolis: Sams Publishing), 18.

[6] Military and Aerospace Electronics, “Crypto Modernization Transforms Military Communications,” last modified 1 December 2011, http://www.militaryaerospace.com/articles/print/volume-22/issue-12/special-report/crypto-modernization-transforms-military-communications.html

[7] Defense Standardization Program, “International Standardization Documents,” last accessed 23 April 2018, http://www.dsp.dla.mil/Specs-Standards/International-Standardization-Documents/

[8] NATO Standardization Office, “Consultation Command and Control Board,” last accessed 23 April 2018, http://nso.nato.int/nso/

to ensure that the hardware and software of current generation systems are interoperable and support technological convergence with the fortress security model.

These structures have worked adequately in the past; however, with recent disruptive advances in modern computing[9] and cryptography,[10] and the desire for nations to maintain national sovereignty over their own information protection capabilities, there is more pressure for technical standardization to federate than ever before.[11] In a federated model, cryptography is still centrally managed for interoperability standardization, but greater autonomy can be achieved at the national or participant level to build compatible hardware and software to a pre-authorized standard. Even with the risk of these disruptive technologies and desire to introduce sovereign cryptographic capabilities, fortress security remains the design architecture favored by the defence sector.

Ironically, the greatest risk to cryptographic interoperability in the NATO alliance is not technical in nature, rather it is the lack of consensus on what modernized cryptographic systems will be procured, and when they will be implemented. This ambiguity has resulted in variances in capability development and integration timelines between distinct Communities of Interest (COI) within NATO.[12] With a lack of consensus in determining a common computing platform, the distributed fortress security model is increasingly under pressure to marginalize security in order to maximize multinational functionality and to reduce hardware costs.

The complex problem of cryptographic standardization on the scale of the NATO alliance may be expected due to the broad range of COIs and stakeholders with different requirements.

[9] Daniel Bernstein, *Post Quantum Cryptography* (Heidelberg, Springer-Verlag, 2009), 16.

[10] Imran Bashir, *Mastering Blockchain* (Birmingham: Packt Publishing, 2018), 8.

[11] United Kingdom, *National Cyber Security Strategy 2016-2021* (London : Cabinet Office, 2017), 51.

[12] Konrad Wrona, *A Common Approach to the Integration of Object Level Protection in NATO* (The Hague: NCI Agency, 2014), 1.

That said, even within small closely aligned alliances, technical interoperability challenges for fortress security and cryptography exist. According to a report generated by the AUSCANNZUKUS MIW Supervisory Board (SB), recent allied experimentation in next generation networking and cryptography was hindered by conflicting national cryptographic objectives and strategies;

> There were specific Allied/Coalition cryptographic device interoperability issues that had to be addressed in order to interconnect [national architectures] and establish the [network]…it was ascertained that there was no common military-grade, Type 1 Internet Protocol encryption device readily available for use within all AUSCANNZUKUS nations.[13]

This is a recent example of how even within a heavily integrated and highly interoperable COI like the AUSCANZUKUS MIW organization; cryptography was still a weak link in achieving the baseline common computing environment that is essential for cyber security standardization and cyber defence operations in the fortress security model. With the increasing complexity and costs associated to maintaining cryptographic interoperability in the fortress model, new technologies are being examined to replace or at least supplement current technology.

[13] US Office of the Chief of Naval Operations, "AUSCANNZUKUS MIW Experimentation Report 2017," (Washington: Office of the Chief of Naval Operations, 2018), 27.

NATO is supporting the development of one of these new technologies in accordance with the Connected Forces Initiative (CFI) through Federated Mission Networking (FMN).[14] It is built on the principle that the requirement for common computing environments that support fortress security (physical hardware and interoperable gateway cryptographic devices) will not be relevant in the future, as encryption and security will be able to be integrated at the data level and will be able to function independent of isolated network boundaries and specialized hardware. In Konrad Wrona's article on Object Level Protection (OLP), he suggests that fortress security will not be the common approach to next generation cryptography and baseline cyber security.[15] He suggests that OLP will replace the need for bespoke cryptographic devices in the future.[16] In this proposed construct, the fundamentals of cyber security encompassing confidentiality, integrity and authentication will be achieved directly at the data object level within a national and multinational network environment. In theory, OLP represents an elegant solution to a complex problem and recently, it has received more prominence in the multinational interoperability community. Rather significantly, the technology was demonstrated at sea in an experimental network environment during Exercise JOINT WARRIOR 2017 through the Canadian Technical Interoperability in a Data Centric Environment (TIDCE) program.[17] It has also been successfully demonstrated in a lab environment through the Coalition Warrior Interoperability eXercise (CWIX) sponsored by NATO Allied Command Transformation (ACT).[18]

[14] NATO Allied Command Transformation, "Federated Mission Networking," last accessed 7 May 2018, http://www.act.nato.int/fmn

[15] Fortress security is the current preferred standard for protecting network interconnections through rigid segregation and gateway defenses.

[16] Konrad Wrona, *A Common Approach to the Integration of Object Level Protection in NATO* (The Hague: NCI Agency, 2014), 1.

[17] US Office of the Chief of Naval Operations, "AUSCANNZUKUS MIW Experimentation Report 2017" (Washington: Office of the Chief of Naval Operations, 2018), 119.

[18] More information on CWIX is available at the following link http://www.act.nato.int/cwix

Even with the technical successes OLP has achieved, the reality is that broad based multinational support for this type of revolutionary technology has not been embraced and it is unlikely that it will be adopted as a standalone cryptographic solution in the short term.[19] This is an example of how technical innovation still needs to overcome multinational sovereignty biases in an increasingly complex and risk adverse cyber security environment that is still heavily influenced by consensus based development. This is not to say that technologies like OLP should not be considered as viable alternatives to traditional fortress security, but rather to say that in the short term a balanced strategy to integrate both traditional fortress security and data centric security should be adopted by those nations with the technical capacity to do so. In the interim, this balanced approach will provide a capability for cryptographic defense in depth and mitigate some of the sovereignty concerns associated with national security caveats in a multinational environment.

In summary, it is clear that there exists a need to maintain and advance fortress security technologies and baseline system interoperability well into the future, even as technologies like OLP mature. For this reason, cryptographic interoperability will remain a complex problem involving multiple stakeholders and including significant technical challenges. That said these challenges can be overcome by balancing operational requirements against the limitations of current cryptographic solutions in meeting the demands of network security supporting network centric warfare.

[19] US Office of the Chief of Naval Operations, “AUSCANNZUKUS MIW Experimentation Report 2017” (Washington: Office of the Chief of Naval Operations, 2018), 119. As an example of national resistance to this new technology, during EX JOINT WARRIOR experimentation, only 1 of 5 nations deployed the TIDCE capability at sea.

A CASE FOR CROSS DOMAIN SOLUTIONS

Interconnectivity, by its very nature introduces cyber security risk by establishing vectors through which unauthorized entry into (and out of) closed networks can be achieved. Deployed naval networks are under increasing pressure to meet the operational requirements for multi-domain interconnectivity while also supporting cyber security standards that enable system assurance in the information warfare domain. The challenge for network architects in the maritime environment is how to find the proper balance between supporting the operator with as much functionality as possible while also ensuring that system integrity can be maintained without accepting unreasonable levels of risk. Fortunately, the operational requirements for interconnectivity have driven innovation in supporting cross domain information exchange technology.

Modern naval platforms have sophisticated network architectures that support platform control functions for propulsion and power generation, combat systems management and a mix of operational and enterprise networks that support classified and unclassified processing to a strategic rear link via satellite communications or other bearers.[20] These systems exist in different security domains and traditionally have been designed to operate in isolation. The current trend in network design, however, is to connect networks to improve automation functions and streamline information exchanges to improve operator functionality in a network centric environment.[21] This change is occurring in an era when the potential of cyber intrusion or attack is consistently increasing.[22] While these types of interconnected architectures are not

[20] Richard Bensing, “An Assessment of Vulnerabilities for Ship Based Controlled Systems,” (thesis, Naval Post Graduate School, 2009), 35.

[21] Department of Defence, *Network Centric Warfare Report to Congress* (Washington, DC: US Government Printing Office, July 27 2001), 2-4.

[22] Lionel Alford, “Cyber Warfare: Protecting Military Systems” Acquisition Review Quarterly (Spring 2000): 102. http://www.dtic.mil/dtic/tr/fulltext/u2/a487951.pdf

desirable from a cyber security point of view, they have, nonetheless, been widely adopted as a means of improving functionality and information exchange.

The requirements for increased system interconnectivity are growing in the maritime domain, largely due to new operational requirements to expand connectivity. One of the most dynamic cross domain information exchange requirements facing network architects is related to Recognized Maritime Picture (RMP) management that support a variety of outputs including; Over the Horizon Targeting Gold (OTH-G) messaging for the Global Command and Control System-Maritime (GCCS-M), LINK 16 Joint Range Extension Applications Protocol – C (JREAP-C) and the NATO Friendly Force Information (NFFI) exchange protocol. These protocols are designed to be exchanged across satellite communications bearers (via operational and enterprise IP networks) but are integrated in some cases directly into platform level control networks called Battle Management Systems (BMS) or Command Management Suites (CMS). This means that information exchanges have to occur between two network architectures with different security classifications and completely different functions. In the case of platform level CMS networks, critical isolated systems for sensors, weapons and navigation are all potentially exposed to an external network. The same problem exists for other platform networks for propulsion, power generation and control systems normally associated to SCADA systems. While this level of interconnectivity increases cyber security risk, new technical solutions that enhance security have also been developed. [23]

The current method in mitigating cyber security risk in a data transfer between two closed systems is through a combination of three distinct capabilities; to minimize the number of transfer gateways, to monitor what traffic is passing through a gateway against a defined baseline

[23] Scott Smith, “Shedding Light on Cross Domain Solutions,” last modified 6 November 2015, 7. https://www.sans.org/reading-room/whitepapers/dlp/shedding-light-cross-domain-solutions-36492

and to control gateway access in the event of a security breach between networks.[24] This combination of capabilities for gateway protection is known as a cross domain solution.[25] Cross domain solutions incorporate some of the traditional security features from the Bell-LaPadula Model for access control and the Clark Wilson Model for system integrity, but are less rigid in their application of security controls and allow for the assumption of risk by a network operational authority.[26] The ability of an operational commander to assume risk on a network architecture is what separates cyber operations from cyber security. It is for this reason that cross domain solutions have become the architectural preference for defence related network operations and particularly for use in complex multinational environments.

Even if the technical complexities of implementing a cross domain solution can be overcome, network architects must also consider the impact of interconnectivity on system authorities, especially if the connected networks have different operational or technical authorities. Cyber defence operations rely on structured decision support mechanisms between technical authorities, security authorities and operational authorities.[27] While these authorities can be easily defined for one network in isolation, the interconnection of many networks can result in very complex decision making and risk assumption structures that are incongruent to the command and control principles supporting cyber defence operations.

In countering this notion that existing security controls and risk management could provide adequate protection for interconnected networks in a contested cyber environment, we must consider the possibility that security mechanisms fail. If complex security controls between

[24] In this context, control of gateway access means the ability to isolate networks in the event of a security breach to prevent proliferation of a threat or the exfiltration of data.

[25] Scott Smith, “Shedding Light on Cross Domain Solutions,” last modified 6 November 2015, 4. https://www.sans.org/reading-room/whitepapers/dlp/shedding-light-cross-domain-solutions-36492

[26] Ibid., 4.

[27] Great Britain House of Commons Defence Committee, *Defence and Cyber-Security: Sixth Report of Session 2012-2013*, (London: The Stationery Office, 2013), 16.

IT systems and SCADA systems fail, there could be catastrophic impacts that no level of risk management can mitigate. In his book *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*, Tyson MacCauley discusses why the risk to connecting IT systems to SCADA and DCS networks has increased significantly in the last decade. His rationale is that new demands for interconnectivity have outpaced the rate of cyber security advances in SCADA control networks. He suggests that while sophisticated defenses and tools to defend against cyber attacks have been developed for enterprise IT networks, the same cannot be said for SCADA networks. He advocates that there is a level of cyber security immaturity for SCADA systems that make the potential connection to sophisticated IT systems very risky from a cyber security perspective.[28]

Keith Stoffer in *The Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) Security* offers another perspective on the cyber security of SCADA networks and presents a case for why they should not be treated in the same manner as a traditional IT network. He suggests that SCADA and ICS [platform] systems directly interface with sensors and machinery and as a result can pose a threat of actual physical damage to the environment in which they exist. He proposes that risk tolerance on SCADA and ICS systems should be lower than what is traditionally accepted on other IT platforms, due to potential real world implications of system manipulation on production networks. His research also highlights some of the complexities that arise in SCADA systems in the conduct of routine activities like

[28] Tyson Macaulay, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*, (Boca Raton : CRC Press 2012), 2.

system re-boots and vulnerability scanning that can result in unexpected outcomes on platform systems.[29]

Both Stoffer and MacCauley provide valid arguments as to why interconnectivity between enterprise and platform networks is dangerous, but their arguments are biased toward security over the functionality demanded by system users. In the modern defence environment, it is the operator who demands functionality, therefore, strategies that balance inherent security provided by security authorities and risk mitigation provided by operational authorities must be adopted in the development of next generation networks. It is easy to image a worst case scenario, whereby a ships propulsion plant is able to be controlled remotely by a threat actor while conducting a complex low speed manoeuver, but the reality is, with proper security controls and risk mitigation strategies in place, SCADA and other platform systems can be protected from external cyber threats.

Future maritime network architectures will have to be adapted to enable the complex risk mitigation strategies that are characteristic of the current operating environment. The lesson to be learned by network operators is that complex architectures need to be evaluated constantly for potential cyber vulnerabilities whenever changes to baseline configurations are made in any interconnected components. Additionally, system architectures designed for a specific function must incorporate security standards that support the overall strategy for system of systems cyber security. Ultimately, in the era of network centric warfare, a balanced and agile approach to system interconnectivity is possible, but only if interconnectivity is carefully planned by security authorities (cyber security) and competently managed by operational authorities (cyber defence) who understand the risk profiles of the systems they depend on.

[29] National Institute of Standards and Technology, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security (*Gaithersburg, MD: NIST, 2006), 4-7.

This paper provided a summary of some of the challenges associated with network architectural design in a multinational maritime environment characterized by increasing interconnectivity requirements. It highlighted the challenges faced by capability development communities in establishing an appropriate balance between cyber security, interoperability and interconnectivity in developing the next generation of multinational deployable naval networks. It discussed the complex technical nature of cryptographic interoperability in a rapidly evolving domain, and demonstrated that even if new technological solutions can be developed, implementation timelines can be hampered by interoperability restrictions derived from competing interests between COIs. It also examined the potential pitfalls of interconnectivity of dissimilar networks and highlighted the responsibility of network operational authorities to understand the limitations of their security architectures and the importance of having informed and effective risk mitigation strategies. The complex problems presented in this paper can be solved, but they require stakeholder consensus and the development of robust policies to ensure that this system of systems operates in unison toward a common security objective. It is critical that capability developers remain engaged in multinational standardization efforts, while also leveraging cyber security expertise, to be in a position to solve the complex problems associated with future high technology system integration.

BIBLIOGRAPHY

Alford, Lionel "Cyber Warfare: Protecting Military Systems." *Acquisition Review Quarterly (Spring 2000)*: 102. http://www.dtic.mil/dtic/tr/fulltext/u2/a487951.pdf

Bashir, Imran. *Mastering Blockchain.* Birmingham: Packt Publishing, 2018.

Bensing, Richard. "An Assessment of Vulnerabilities for Ship Based Controlled Systems." Thesis, Naval Post Graduate School, 2009.

Bernstein, Daniel. *Post Quantum Cryptography*. Heidelberg: Springer-Verlag, 2009.

Clark, David and Wilson, David. "A Comparison of Commercial and Military Computer Security Policies." *MIT Laboratory for Computer Sciences IEEE* (16 June 1987): 189. https://www.researchgate.net/publication/220713836_A_Comparison_of_Commercial_and_Military_Computer_Security_Policies

Defense Standardization Program. "International Standardization Documents," last accessed 23 April 2018, http://www.dsp.dla.mil/Specs-Standards/International-Standardization-Documents/

Great Britain House of Commons Defence Committee. *Defence and Cyber-Security: Sixth Report of Session 2012-2013*. London: The Stationery Office, 2013.

LaPadula, Len and Bell, Elliott. "Secure Computer Systems: Mathematical Foundations." *MITRE Technical Report 2547, Volume I* (March 1973): 12.

Macaulay, Tyson. *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton : CRC Press, 2012.

Menezes, Alfred. *Handbook of Applied Cryptography*. Boca Raton : CRC Press, 1997.

Military and Aerospace Electronics. "Crypto Modernization Transforms Military Communications." last modified 1 December 2011. http://www.militaryaerospace.com/articles/print/volume-22/issue-12/special-report/crypto-modernization-transforms-military-communications.html

National Institute of Standards and Technology. *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) Security.* Gaithersburg, MD: NIST, 2006.

NATO Allied Command Transformation. "Federated Mission Networking." last accessed 7 May 2018, http://www.act.nato.int/fmn

NATO Standardization Office. "Consultation Command and Control Board." last accessed 23 April 2018, http://nso.nato.int/nso/

Smith, Scott. “Shedding Light on Cross Domain Solutions,” last modified 6 November 2015. https://www.sans.org/reading-room/whitepapers/dlp/shedding-light-cross-domain-solutions-36492

United Kingdom Cabinet Office. *National Cyber Security Strategy 2016-2021.* London : Cabinet Office, 2017.

US Department of Defence, *Network Centric Warfare Report to Congress* (Washington, DC: US Government Printing Office, July 27 2001), 2-4.

US Office of the Chief of Naval Operations. “AUSCANNZUKUS MIW Experimentation Report 2017.” Washington: Office of the Chief of Naval Operations, 2018.

Watson, Jenny. *Maximum Security.* Indianapolis: Sams Publishing, 2003.

Wrona, Konrad. *A Common Approach to the Integration of Object Level Protection in NATO.* The Hague: NCI Agency, 2014.