National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CAPABILITY DEVELOPMENT OF INFORMATION ASSURANCE: STRENGTHENING CANADA'S SOVEIGNTY THROUGH ITS DEFENCE INDUSTRY

Maj Marc Prince

JCSP 43 DL

Exercise *Solo Flight*

Disclaimer

PCEMI 43 AD

Exercice *Solo Flight*

Avertissement

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 43 DL – PCEMI 43 AD
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CAPABILITY DEVELOPMENT OF INFORMATION ASSURANCE: STRENGTHENING CANADA'S SOVEIGNTY THROUGH ITS DEFENCE INDUSTRY

Maj Marc Prince

Word Count: 3271

Compte de mots: 3271

CAPABILITY DEVELOPMENT OF INFORMATION ASSURANCE: STRENGTHENING CANADA'S SOVEIGNTY THROUGH ITS DEFENCE INDUSTRY

INTRODUCTION

Information Assurance (IA) underpins Canada's sovereignty and protects the nervous system of central government by securing communications, thus denying our adversaries access to our most sensitive information and plans. IA is a cornerstone of Canada's autonomy, without it our plans would be known upon conception and our adversaries could exploit or counter these plans prior to their execution. A key component of IA are the Type-1 cryptographic devices that secure federal information and communications between the various departmental facilities of the Government of Canada (GoC), such as those of the Department of National Defence (DND), the Royal Canadian Mounted Police (RCMP), Global Affairs Canada (GAC), and the Communications Security Establishment (CSE). CSE has the GoC mandate to protect Canada's electronic information and computer networks, and one of the means it accomplishes this is by employing Type-1 cryptographic devices, to protect classified information[1]. Within the communications security community, these Type-1 cryptographic devices are also known as High Assurance (HA) technology products, where there are six (6) "major families of devices that are approved by CSE: secure voice devices, network encryptors, link encryptors, secure remote access devices, hard disk encryptors, and tier 3 management devices"[2]. The cryptographic technologies in tactical radios exist on the boundaries between secure voice devices, network encryptors, and link encryptors.

[1] Government of Canada. Communications Security Establishment., "Protecting Canada's Electronic Information and Computer Networks," 2017, https://www.cse-cst.gc.ca/en/inside-interieur/protect-protection.

[2] Government of Canada. Communications Security Establishment., "High Assurance Technology Products," 2014, https://www.cse-cst.gc.ca/en/page/products.

These HA devices protect the production, transmission, and storage of sensitive GoC information such as the annual budget report, intelligence reports between the Canadian Embassies and GAC HQ, and Allied (including NORAD and NATO) plans for troop deployment into Theatres Of Operation (TOO). As an example within the Canadian Armed Forces (CAF), these devices protect the information of both the location and time of arrival and departure of military aircraft or, in the case of our Allies, the port of calls (times of arrival/departure) of naval assets such as US Inter-Continental Ballistic Missile (ICBM) submarines. Compromise of these communications would enable the adversaries of Canada (and its Allies) to exploit the information for economic gain or to disrupt (or destroy) Canadian (and Allied) forces.

While Canada has in the past produced a small quantity of HA devices, most have been obtained from the US. In 2005, the TBS approved $839M Cdn for the Canadian Cryptographic Modernization Program (CCMP) Omnibus Project[3]. This is a 12 year project, of which no Industrial Regional Benefits (IRBs) were originally scheduled to be assigned to Canadians. However, in 2014, General Dynamics Canada announced that it had been awarded $122M Cdn to enhance DND's combat radios which had originally been procured in 1991[4]. Enabled by the defence development sharing agreement between Canada and the US[5], the bulk of the funds (approximately 85%) were thus invested into the US defence industry. In 2017, DND reconfirmed that there were no IRBs associated with CCMP[6] which it stated would now close

[3] Government of Canada. Department of National Defence, "Departmental Performace Report 2007-08: Table 5: Status Report on Major Crown Projects," *Departmental Performance Reports* (Ottawa, ON, Canada, 2008), https://www.tbs-sct.gc.ca/dpr-rmr/2007-2008/inst/dnd/st-ts05-eng.asp#t5-06.

[4] General Dynamics. Mission Systems Canada, "General Dynamics to Upgrade Canadian Army's Combat Net Radios," 2014, https://www.gd-ms.ca/news/general-dynamics-to-upgrade-canadian-army's-combat-net-radios.html.

[5] Government of Canada. Industry Canada, "Defence Development Sharing Agreement between Canada and the United States of America," 2014, https://www.ic.gc.ca/eic/site/ad-ad.nsf/eng/ad01691.html.

[6] Government of Canada. Department of National Defence, "Department of National Defence and the Canadian Armed Forces - 2017-18 Departmental Plan. Status Report on Transformational and Major Crown

out in 2021. Looking into the future, the 2016 Defence Acquisition Guide (DAG) advertises that the Army is standing up the Land Command Support System Tactical Communication Modernization project with an upper estimate of $1.5B Cdn[7], with a contract award date of 2022 and final delivery in 2036 (spanning 14 years). This represents an opportunity for Canadians to capture a market share of the cryptographic industry. In addition, the greater DND (and GoC as a whole) requirements, while undisclosed, would reasonably be expected to dwarf the expenditures of the Army.

With the fragility of our dependence on the US being brought to light by the current volatility of the Trump Administration, Canadians are seeking to reduce our dependency on the US by diversifying our export markets in oil (with the Kinder Morgan Trans Mountain Pipeline[8]) and lumber (with new exports to China[9]). Of particular concern are the recent indications that the Trump family were in direct cooperation with the Russian government to assist President Trump in seizing control of the presidency[10]. With alliances apparently shifting in this age of globalization, Canada has to be prepared to diversify the source of its HA devices should the US continue to follow its current path and decide to use its HA export policies as leverage to achieve other import or export objectives. To reduce our dependence on the US, the conditions must be in place for Canadian industry to take on the role for the development and manufacturing of HA capabilities. While progress has been made with national policies and programs to encourage the

---

Projects: Canadian Cryptographic Modernization Program," 2017, http://www.forces.gc.ca/en/about-reports-pubs-report-plan-priorities/2017-status-report-on-transformational-and-major-crown-projects.page#p4.

[7] Government of Canada. Department of National Defence, "Defence Acquisition Guide 2016. Land System Services: Land Command Support System Tactical Communications Modernization," 2016, http://www.forces.gc.ca/en/business-defence-acquisition-guide-2016/land-systems-93.page.

[8] Steven Maher, "Justin Trudeau Is Going to Have to Buy Himself a Pipeline," *Maclean's*, 2018, http://www.macleans.ca/opinion/justin-trudeau-is-going-to-have-to-buy-himself-a-pipeline/.

[9] Mike Blanchfield, "Trade Minister Courts China for Softwood as US Announces Duties on Canadian Lumber," *CBC News*, 2017, http://www.cbc.ca/news/politics/canada-china-softwood-market-1.4085269.

[10] BBC, "Trump-Russia 'Collusion: Democrats File Lawsuit," *BBC*, 2018, http://www.bbc.com/news/world-us-canada-43844253.

Canadian defence industry, these have not been sufficient to precipitate a viable IA industry within Canada, particularly in the production of HA devices. This paper will evaluate the Canadian Government's policies and programs to determine which conditions are in place to foster an HA industry in Canada and where improvements to these would promote economic development of this important defence sector. The policies to be examined relate to the alignment with our allies in the export of arms (the Wassenaar Arrangement and the Arms Trade Treaty), to the strengthening of industrial benefits to Canadian companies (Industrial and Technological Benefits and the Controlled Goods Program), and further enhancements to the CSE cryptography program (Cryptographic Algorithm and Module Certification Programs).

ALIGNMENT WITH INTERNATIONAL EXPORT LAWS

The first activity to promote a cryptographic industry on Canadian soil is to align our policies with those of the International Community with respect to the exports of arms. In order to be aligned, Canada needs to ensure that the Canadian Controlled Goods Program (CGP) is aligned with the Wassenaar Arrangement[11] (WA) and that Canada signs onto the Arms Trade Treaty[12]. Both of these are required to gain the trust of the other nations that are producing and exporting cryptographic technologies. Without being members of these two agreements, Canada places itself in the same class as China, Russia, and Iran, which are often perceived as industrialists of war capabilities, profiting from the sale of arms at the expense of human misery. Nations that have signed onto the Arms Trade Treaty are unwilling to deal with those that have

[11] Wassenaar Arrangement Secretariat, "The Wassenaar Arrangement: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies," 2017, https://www.wassenaar.org/.

[12] The United Nations Office For Disarmament Affairs (UNODA), "The Arms Trade Treaty," *UNODA*, 2013, https://www.un.org/disarmament/att/.

not for fear that any arms technologies exported to these non-signatory nations would simply be resold for profit.

Thankfully Canada has matched (almost word for word) its export list to that of the Wassenaar Arrangement. Category 5 – Part 2 – "Information Security"[13] of the WA is concerned with the sale of cryptographic capabilities. Similarly, Global Affairs Canada has published "A Guide To Canada's Export Control List" which details cryptographic capabilities in Group 1 – Dual-Use List – Category 5 – Part 2: "Information Security"[14]. A close comparison of the two documents reveals that Canada's Export Control List is a very close adaptation of that of the Wassenaar Arrangement. This synchronization with the WA is particularly important for Canadians seeking to enter into joint venture with either our US or UK allies (or other allies) in the development of HA capabilities.

The US, a founding member of the WA, has aligned their Export Administration Regulation with that of the WA. Category 5 Part 2 – Information Security of their Commerce Control List[15] very closely matches that of the WA. The Commerce Control List is an extrapolation of the US International Traffic in Arms Regulations[16] (ITAR) which also provides the framework for licensing procedures, import of classified materiel (through Technical Assistance Agreements) and the conditions under which nationally manufactured equipment can

---

[13] Wassenaar Arrangement Secretariat, *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Volume II List of Dual-Use Goods and Technologies and Munitions List*, vol. II (Vienna, Austria: Wassanaar Arrangement Secretariat, 2017). p. 91-97.

[14] Global Affairs Canada Trade Control Bureau, *A Guide To Canada's Export Control List* (Ottawa, ON: Government of Canada, 2015), http://www.international.gc.ca/controls-controles/assets/pdfs/documents/guide-2015-eng.pdf. p. 77-82.

[15] Bureau of Industry and Security. U.S. Department of Commerce., *Export Administration Regulation: Commerce Control List* (Washington, DC: U.S. Department of Commerce, 2017), https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear. p. 1-11.

[16] United States Government Department of State, *The International Traffic in Arms Regulations (ITAR): Part 121 — The United States Munitions List* (Washington, DC, USA: Department of State, 2018), http://www.pmddtc.state.gov/regulations_laws/itar.html. p.480

be re-export to 3rd party nations[17]. While closer collaboration with the US might seem counter-intuitive to increasing Canada's sovereignty, it would enable the manufacturing of HA devices on Canadian soil. In effect a deeper Canada-US partnership would promote a more balanced relationship, where it is currently one-sided towards US development, manufacturing and export.

Similarly, the UK has also aligned their Strategic Export Control List – Category 5 – Part 2 – "Information Security"[18] to that of the WA. While Canada has not imported significant UK manufactured HA devices, the fact that both Canada and the UK have harmonized export control lists lends to future collaboration on the development and production of cryptographic devices. A key advantage to collaborating with the UK is the fact that procurement of cryptographic equipment would not fall under the US ITAR regulations, where these have significant bureaucratic overhead associated with them. But it remains to be determined whether the UK can offer the full range of cryptographic equipment currently available from the US.

While Canada has aligned itself with its Allies in recognizing technologies for restricted export, it remains misaligned with respect to the clients to whom it exports. This is the foundational concept of the Arms Trade Treaty[19] (ATT) which originated with the United Nations Office for Disarmament Affairs[20] (UNODA) and entered into force in December of 2014. The ATT seeks to restrict the sale and export of arms to nations that violate the law of armed conflict or that have a blatant disregard for human rights. Concerned with the impact to

---

[17] United States Government Department of State, *The International Traffic in Arms Regulations (ITAR): Part 125 — Licences for the Export of Technical Data and Classified Defence Articles* (Washington, DC: Department of State, 2018), http://www.pmddtc.state.gov/regulations_laws/itar.html. p.532-535.

[18] Department for International Trade. UK Government., *UK Strategic Export Control Lists* (London, UK: UK Government, 2018), https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation. p. 10-15

[19] The United Nations Office For Disarmament Affairs (UNODA), "The Arms Trade Treaty."p.2-3.

[20] The United Nations, "The United Nations Office for Disarmament Affairs (UNODA): About Us," 2018, https://www.un.org/disarmament/about/.

Canadian firearms owners, the legacy Harper Government was cautious in signing the ATT[21]. As such, Canada remains one of the few countries that has withheld commitment to join its Allies in restricting the sale of arms to nations known to violate human rights. An example of the type of controversy that can surround the export of arms is the recent "$15 billion deal to sell light armoured vehicles to Saudi Arabia, which has been repeatedly criticized by human rights groups"[22].

To address this misalignment, the Liberal Government has proposed Bill C-47 which aims to amend both the Export and Import Permits Act and the Criminal Code of Canada to set the conditions for Canadian accession to the ATT[23]. The bill has come under criticism from human rights groups as it does not restrict the export of arms to the United States, which has only signed the ATT and not ratified it. The significance of this can be seen through the example where Canadian manufactured engines were integrated into US military aircraft and then resold to Nigeria (which has a history of human rights abuses)[24]. As nearly 50% of Canada's arms exports flow to the US, Canadians are obviously concerned with being guilty through third party association with foreign arms manufacturers and distributors[25]. This problem could be solved once the US ratifies the ATT, and while not an objective of the Trump Administration (which lifted the ban set by the previous Obama Administration to export military aircraft to Nigeria), it

---

[21] Robert Fox, "Oped: Canada's Strange Inaction on the Arms Trade Treaty," *Ottawa Citizen*, no. 24 September (2014), http://ottawacitizen.com/news/national/canadas-strange-inaction-on-the-arms-trade-treaty.

[22] Murray Brewster, "Canada to Join Global Arms Trade Treaty under Legislation Tabled Thursday," *CBC*, no. April (2017), http://www.cbc.ca/news/politics/arms-trade-treaty-1.4070539.

[23] Government of Canada. Global Affairs Canada, *HOUSE OF COMMONS OF CANADA - BILL C-47 - An Act to Amend the Export and Import Permits Act and the Criminal Code (Amendments Permitting the Accession to the Arms Trade Treaty and Other Amendments)* (Ottawa, ON, Canada: Government of Canada, 2018), http://www.parl.ca/DocumentViewer/en/42-1/bill/C-47/second-reading.

[24] Marie-Danielle Smith, "Federal Liberals Strengthen Arms Exports Bill but Experts Say Big Loopholes Remain," *National Post*, no. March (2018), http://nationalpost.com/news/politics/federal-liberals-strengthen-arms-exports-bill-but-experts-say-big-loopholes-remain.

[25] Lucas Powers, "Canadian Arms Trade Much Larger than Data Suggests, Expert Says," *CBC News*, no. February (2016), http://www.cbc.ca/news/business/canada-arms-technology-trade-1.3458608.

is assumed that this is a long term goal of the American people. With or without the US, those signatories of the ATT can trust that arms sold to each other will not be resold to nations that would use them in ways contrary to the intent of the ATT. This effectively forms a trusted group of nations with a common belief on the use of armed force and the export of the tools to enable it. Bill C-47 will permit Canada to join this trusted group of nations and with it new partnerships and possibilities to collaborate on developing and manufacturing new technologies, such as Information Assurance (and HA devices). Thus, accession to the ATT would provide Canada with the opportunity to diversify its partnerships in the development, manufacturing, and export of HA devices, thus greatly increasing the market for Canadian industry.

STRENGTHENING INDUSTRIAL BENEFITS

There are three main avenues to encourage Canadian industry to produce HA devices to meet the needs of the GoC. The first is to inform them of the long term requirement within the GoC, the second is to divert funding to these Canadian industries (as opposed to funding US industries), and the third is to structure the contracts so that Canadian businesses can afford to bid on them.

The Jenkins report of 2013 recommended the creation and communication of Key Industrial Capabilities (KICs) to forewarn Canadian Industry of future defence requirements, thus giving them time to adjust their capability development and manufacturing to meet the needs of the CAF[26]. What has since emerged is the annual Departmental Plan where the 2018-19 plan details the total annual funding envelopes (multi-year) for the procurement of defence

[26] Tom Jenkins, *Canada First: Leveraging Defence Procurement through Key Industrial Capabilities*, 2013. p. ix-x.

capabilities[27]. Providing further detail on each of the major capital investment programs, DND produced the Defence Acquisition Guide (DAG) and Industry Canada published the Industrial and Technological Benefits (ITB), where these lists provide even more information on the individual procurement projects[28].

Closer examination of these lists reveals that each of the projects are largely focused on force developing a specific platform. Understandably, platforms are easier to comprehend as they provide a tangible asset for the project to deliver and are much simpler to communicate, as an actual deliverable, to both politicians and the Canadian taxpayer. While this form of project structure (herein after referred to as the platform procurement model) offers advantages for gaining support for the capability, it has a three major disadvantages.

The first disadvantage is the exorbitant cost associated with a platform project; where only a prime contractor has the financial means to submit a bid. Most prime contractors are US based companies that have established satellite offices in Canada. The only opportunity for Canadian Small and Medium sized Enterprises (SMEs) are to be employed through a sub-contract from the US prime contractor. Sub-contracts are directed by the prime contractor and they usually favour known entities with whom they have employed in the past. This generally means that US based prime contractors will direct their sub-contracts to the US based companies with whom they have formed previous business partnerships. As the production of HA devices is limited to a closely knit group of US companies, there is very little opportunity to naturally grow that industry here in Canada. The solution to these long established relationships is the deliberate

[27] Government of Canada. Department of National Defence, "Department of National Defence and the Canadian Armed Forces - 2018-19 - Departmental Plan" (Ottawa, ON, Canada, 2018), http://www.forces.gc.ca/en/about-reports-pubs-report-plan-priorities/2018-index.page. p.40.

[28] Government of Canada. Industry Canada, "Industrial and Technological Benefits: Procurement Projects," 2018, http://www.ic.gc.ca/eic/site/086.nsf/eng/h_00056.html.

direction of funding envelopes, within the IRBs, targeted towards specific technology manufacturing (such as HA devices) on Canadian soil. Public Services and Procurement Canada (PSPC) could assist with this effort, as it is responsible for the Controlled Goods Program[29] (inherited through the Defence Production Act[30]), by engaging its Washington Office (collocated with the GAC embassy) to direct US industry to sub-contract to Canadian companies in manufacturing these HA devices.

The second disadvantage is unique to the business of communications in that the platforms all need to interoperate with each other. The concept used to describe this force development stream is known as a System-of-Systems (SoS) approach. With the current platform procurement model, communications equipment (and the HA modules that secure them) are all procured separately within the confines of each platform with little regard given to interoperability between the various platforms. While this initially meets the requirement of the platform project, it creates a hodgepodge of communications and encryption technologies which vary in degrees of interoperability, and unfortunately are only able to securely communicate with each other in the simplest ways (typically voice only).

The third disadvantage of the platform procurement model is the fact that the total cost (and thus requirements) of HA expenditures remains ambiguously hidden within the cost of each platform project. Thus, Canadian industry has no way of knowing the total investment associated with HA devices. Without this knowledge, Canadian industry cannot focus on a particular HA technology that would bring the greatest Return On Investment (ROI) and thus be a sustainable long term business investment.

---

[29] Government of Canada. Public Works and Government Services Canada, "Controlled Goods: Examining, Possessing or Transferring," 2018, https://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html.

[30] Minister of Justice Government of Canada, *Defence Production Act* (Canada, 2017), http://laws-lois.justice.gc.ca/PDF/D-1.pdf. p.2-5.

The current situation with the platform procurement model can be solved by centralizing the procurement of communications and encryption technologies under an omnibus program; this would consist of several independent projects (and contracts) each designed to field a specific HA device. This would bring the full scope of Canada's requirement under one umbrella and break up the costs sufficiently so that any given Canadian SME could both focus their efforts on delivering one of the HA devices and afford to compete for one of the projects. It would also permit the GoC to direct IRBs to these specific contracts, thus promoting Canadian investment in the production of HA devices. A positive second order effect would be to promote greater interoperability between the four services (Navy, Army, Air Force, and SOF) of the CAF.

STRENGTHENING THE CSE CRYPTOGRAPHY PROGRAM

As the GoC lead agency on HA devices, CSE has two key programs to encourage the development of High Assurance technologies, these are the Cryptographic Algorithm Validation Program[31] (CAVP) and the Cryptographic Module Validation Program[32] (CMVP). CSE has also partnered with the National Institute of Standards and Technology (NIST) for the joint management of the equivalent US CAVP[33] and CMVP[34]. Both of these programs aim to assist Canadian industry in the development of cryptographic technologies and are quite relevant as

[31] Government of Canada. Communications Security Establishment., "Cryptographic Algorithm Validation Program (CAVP)," 2014, https://www.cse-cst.gc.ca/en/page/cavp.

[32] Government of Canada. Communications Security Establishment., "Cryptographic Module Validation Program (CMVP)," 2017, https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program.

[33] National Institute of Standards and Technology (NIST). Computer Security Resource Center., "Cryptographic Algorithm Validation Program," 2018, https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program.

[34] National Institute of Standards and Technology (NIST). Computer Security Resource Center., "Cryptographic Module Validation Program," 2018, https://csrc.nist.gov/projects/cryptographic-module-validation-program/module-validation-lists.

more HA devices use the FIPS 140-2 security specification[35]. As the support of the GoC exists within these two programs, the conditions appear to be nearly in place to encourage Canadian industry to manufacture HA devices; however, two components are missing. The first component involves increasing the scope of the programs to include HA devices and the second is focusing Canadian industry onto a particular HA technology. The first would involve expanding the existing policies to include HA devices and allocating funding to cover the additional resources to manage the program. The second missing component is the identification of a major family of HA devices that would generate the highest ROI for Canadian industry. As CSE brokers the procurement of all HA devices, it has the insight to guide industry to manufacture those HA devices that are (or will be) in highest demand within the GoC (and the international community).

The CSE web sites on available training courses[36] and the various policy manuals reveals that the GoC utilizes the following HA devices (organized by HA family):

a. Secure Voice Devices. Secure Terminal Equipment[37] (STE);
b. Network Encryptors. The TACLANE Micro Encryptor and GEM X[38];
c. Link Encryptors. KIV-7M[39];
d. Secure Remote Access Devices. KOV-26 Talon[40];
e. Hard disk encryptors. Eclypt[41];
f. Tier 3 Management Devices. AN/PYQ-10 - Simple Key Loader[42] (SKL).

---

[35] Government of Canada. Communications Security Establishment., "What Is FIPS 140?," 2014, https://www.cse-cst.gc.ca/en/page/what-fips-140.

[36] Government of Canada. Communications Security Establishment., "Information Technology Security Learning Center - Course List," 2018, https://www.cse-cst.gc.ca/en/learning/course/list.

[37] L-3 Communication Systems-East, "Secure Terminal Equipment," 2018, http://www2.l3t.com/cs-east/what-we-do/products/encryption-products_secure-terminal-equipment.htm.

[38] General Dynamics. Mission Systems, "TACLANE-Micro (KG-175D) Encryptor," 2018, https://gdmissionsystems.com/products/encryption/taclane-network-encryption/taclane-micro-kg-175d-encryptor.

[39] Metrodata, "KIV-7M," 2007, http://www.metrodata-defense.com/crypto/safenet-mykotronx/kiv-7m.html.

[40] L-3 Communication Systems-East, "Talon - Small Form-Factor/Portable Encryption," 2018, http://www2.l3t.com/cs-east/what-we-do/products/encryption-products_talon.htm.

[41] Viasat, "Eclypt Core Encrypted Internal Hard Drive," 2018, https://www.viasat.com/products/encryption-eclypt-core.

All of these devices are exported from the US to Canada, where only the Eclypt has its origins in the UK[43]. With the current move towards networking and Voice over IP (VoIP), Canadian industry would be well advised to focus HA development within the family of Network Encryptors. To support this effort, CSE would need to expand the scope of the CMVP to include network encryptors, thus significantly limiting the size of the government investment in this program and the associated risk. In addition, CSE could look to expand its partnership beyond the US to include the UK, where the later is manufacturing its own HA devices, such as the Common Core Crypto Module, which is "unencumbered by ITAR"[44].

CONCLUSION

In conclusion, the conditions are still not in place for Canadians to produce their own Higher Assurance devices and thus the sovereignty of Canada remains underpinned by its relations with the USA. However, the GoC could achieve a greater state of sovereignty by setting the conditions for Canadian industry to produce High Assurance devices here in Canada. The GoC can accomplish this by further aligning itself with its international allies, by strengthening its industrial benefits, and by further investing in its government sponsored cryptographic program. First, Canada needs to ratify the Arms Trade Treaty, further aligning it with its allies, with the outcome of significantly expanding the cryptographic market through a broader base of trusted export partners. Second, Canada needs to centralize its cryptographic requirements,

---

[42] Sierra Nevada Corporation, "AN/PYQ-10 SKL v3.1," 2018, https://www.sncorp.com/media/2400/eis_cns_an-pyq-10-skl-v31-product-sheet_2-23-18_reduced.pdf.

[43] J.E. Dunn, "Encryption Company Stonewood Bought by ViaSat," *NetworkWorld*, 2010, https://www.networkworld.com/article/2211324/security/encryption-company-stonewood-bought-by-viasat.html.

[44] Ultra Electronics Communications & Integrated Systems, "COMMON CORE CRYPTO MODULE COMSEC BOUNDARY OF MODERN LINK ENABLED CRYPTOGRAPHIC DEVICES," 2017, https://www.ultra-cis.com/capabilities/encryption/military-crypto#download-modal-form. p.1

produce smaller tender packages, and direct IRBs thus ensuring that Canadian industry are competitive and receive contracts to manufacture HA devices on sovereign soil. Finally, Canada needs to further invest in CSE's CMVP, expanding its mandate and international partnerships to develop HA devices from the family of Network Encryptors, which will ensure the greatest ROI for Canadian industry.

BIBLIOGRAPHY

BBC. “Trump-Russia ’Collusion: Democrats File Lawsuit.” *BBC*, 2018. http://www.bbc.com/news/world-us-canada-43844253.

Blanchfield, Mike. “Trade Minister Courts China for Softwood as US Announces Duties on Canadian Lumber.” *CBC News*, 2017. http://www.cbc.ca/news/politics/canada-china-softwood-market-1.4085269.

Brewster, Murray. “Canada to Join Global Arms Trade Treaty under Legislation Tabled Thursday.” *CBC*, no. April (2017). http://www.cbc.ca/news/politics/arms-trade-treaty-1.4070539.

Bureau of Industry and Security. U.S. Department of Commerce. *Export Administration Regulation: Commerce Control List*. Washington, DC: U.S. Department of Commerce, 2017. https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

Defence, Government of Canada. Department of National. “Department of National Defence and the Canadian Armed Forces - 2018-19 - Departmental Plan.” Ottawa, ON, Canada, 2018. http://www.forces.gc.ca/en/about-reports-pubs-report-plan-priorities/2018-index.page.

Department for International Trade. UK Government. *UK Strategic Export Control Lists*. London, UK: UK Government, 2018. https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation.

Department of State, United States Government. *The International Traffic in Arms Regulations (ITAR): Part 121 — The United States Munitions List*. Washington, DC, USA: Department of State, 2018. http://www.pmddtc.state.gov/regulations_laws/itar.html.

———. *The International Traffic in Arms Regulations (ITAR): Part 125 — Licences for the Export of Technical Data and Classified Defence Articles*. Washington, DC: Department of State, 2018. http://www.pmddtc.state.gov/regulations_laws/itar.html.

Dunn, J.E. “Encryption Company Stonewood Bought by ViaSat.” *NetworkWorld*, 2010. https://www.networkworld.com/article/2211324/security/encryption-company-stonewood-bought-by-viasat.html.

Fox, Robert. “Oped: Canada’s Strange Inaction on the Arms Trade Treaty.” *Ottawa Citizen*, no. 24 September (2014). http://ottawacitizen.com/news/national/canadas-strange-inaction-on-the-arms-trade-treaty.

General Dynamics. Mission Systems. “TACLANE-Micro (KG-175D) Encryptor,” 2018. https://gdmissionsystems.com/products/encryption/taclane-network-encryption/taclane-micro-kg-175d-encryptor.

General Dynamics. Mission Systems Canada. “General Dynamics to Upgrade Canadian Army’s Combat Net Radios,” 2014. https://www.gd-ms.ca/news/general-dynamics-to-upgrade-canadian-army’s-combat-net-radios.html.

Government of Canada. Communications Security Establishment. “Cryptographic Algorithm Validation Program (CAVP),” 2014. https://www.cse-cst.gc.ca/en/page/cavp.

———. “Cryptographic Module Validation Program (CMVP),” 2017. https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program.

———. “High Assurance Technology Products,” 2014. https://www.cse-cst.gc.ca/en/page/products.

———. “Information Technology Security Learning Center - Course List,” 2018. https://www.cse-cst.gc.ca/en/learning/course/list.

———. “Protecting Canada’s Electronic Information and Computer Networks,” 2017. https://www.cse-cst.gc.ca/en/inside-interieur/protect-protection.

———. “What Is FIPS 140?,” 2014. https://www.cse-cst.gc.ca/en/page/what-fips-140.

Government of Canada. Department of National Defence. “Defence Acquisition Guide 2016. Land System Services: Land Command Support System Tactical Communications Modernization,” 2016. http://www.forces.gc.ca/en/business-defence-acquisition-guide-2016/land-systems-93.page.

———. “Departmental Performace Report 2007-08: Table 5: Status Report on Major Crown Projects.” *Departmental Performance Reports*. Ottawa, ON, Canada, 2008. https://www.tbs-sct.gc.ca/dpr-rmr/2007-2008/inst/dnd/st-ts05-eng.asp#t5-06.

———. “Department of National Defence and the Canadian Armed Forces - 2017-18 Departmental Plan. Status Report on Transformational and Major Crown Projects: Canadian Cryptographic Modernization Program,” 2017. http://www.forces.gc.ca/en/about-reports-pubs-report-plan-priorities/2017-status-report-on-transformational-and-major-crown-projects.page#p4.

Government of Canada. Global Affairs Canada. *HOUSE OF COMMONS OF CANADA - BILL C-47 - An Act to Amend the Export and Import Permits Act and the Criminal Code (Amendments Permitting the Accession to the Arms Trade Treaty and Other Amendments)*. Ottawa, ON, Canada: Government of Canada, 2018. http://www.parl.ca/DocumentViewer/en/42-1/bill/C-47/second-reading.

Government of Canada. Industry Canada. "Defence Development Sharing Agreement between Canada and the United States of America," 2014. https://www.ic.gc.ca/eic/site/ad-ad.nsf/eng/ad01691.html.

———. "Industrial and Technological Benefits: Procurement Projects," 2018. http://www.ic.gc.ca/eic/site/086.nsf/eng/h_00056.html.

Government of Canada. Public Works and Government Services Canada. "Controlled Goods: Examining, Possessing or Transferring," 2018. https://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html.

Government of Canada, Minister of Justice. *Defence Production Act*. Canada, 2017. http://laws-lois.justice.gc.ca/PDF/D-1.pdf.

Jenkins, Tom. *Canada First: Leveraging Defence Procurement through Key Industrial Capabilities*, 2013.

L-3 Communication Systems-East. "Secure Terminal Equipment," 2018. http://www2.l3t.com/cs-east/what-we-do/products/encryption-products_secure-terminal-equipment.htm.

———. "Talon - Small Form-Factor/Portable Encryption," 2018. http://www2.l3t.com/cs-east/what-we-do/products/encryption-products_talon.htm.

Maher, Steven. "Justin Trudeau Is Going to Have to Buy Himself a Pipeline." *Maclean's*, 2018. http://www.macleans.ca/opinion/justin-trudeau-is-going-to-have-to-buy-himself-a-pipeline/.

Metrodata. "KIV-7M," 2007. http://www.metrodata-defense.com/crypto/safenet-mykotronx/kiv-7m.html.

National Institute of Standards and Technology (NIST). Computer Security Resource Center. "Cryptographic Algorithm Validation Program," 2018. https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program.

———. “Cryptographic Module Validation Program,” 2018. https://csrc.nist.gov/projects/cryptographic-module-validation-program/module-validation-lists.

Powers, Lucas. “Canadian Arms Trade Much Larger than Data Suggests, Expert Says.” *CBC News*, no. February (2016). http://www.cbc.ca/news/business/canada-arms-technology-trade-1.3458608.

Sierra Nevada Corporation. “AN/PYQ-10 SKL v3.1,” 2018. https://www.sncorp.com/media/2400/eis_cns_an-pyq-10-skl-v31-product-sheet_2-23-18_reduced.pdf.

Smith, Marie-Danielle. “Federal Liberals Strengthen Arms Exports Bill but Experts Say Big Loopholes Remain.” *National Post*, no. March (2018). http://nationalpost.com/news/politics/federal-liberals-strengthen-arms-exports-bill-but-experts-say-big-loopholes-remain.

The United Nations. “The United Nations Office for Disarmament Affairs (UNODA): About Us,” 2018. https://www.un.org/disarmament/about/.

The United Nations Office For Disarmament Affairs (UNODA). “The Arms Trade Treaty.” *UNODA*, 2013. https://www.un.org/disarmament/att/.

Trade Control Bureau, Global Affairs Canada. *A Guide To Canada’s Export Control List*. Ottawa, ON: Government of Canada, 2015. http://www.international.gc.ca/controls-controles/assets/pdfs/documents/guide-2015-eng.pdf.

Ultra Electronics Communications & Integrated Systems. “COMMON CORE CRYPTO MODULE COMSEC BOUNDARY OF MODERN LINK ENABLED CRYPTOGRAPHIC DEVICES,” 2017. https://www.ultra-cis.com/capabilities/encryption/military-crypto#download-modal-form.

Viasat. “Eclypt Core Encrypted Internal Hard Drive,” 2018. https://www.viasat.com/products/encryption-eclypt-core.

Wassenaar Arrangement Secretariat. “The Wassenaar Arrangement: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies,” 2017. https://www.wassenaar.org/.

———. *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Volume II List of Dual-Use Goods and Technologies and Munitions List*. Vol. II. Vienna, Austria: Wassanaar Arrangement Secretariat, 2017.