POLITICA DE SECURITATE CIBERNETICĂ A CANADEI

CANADA'S CYBER SECURITY POLICY

Lt.col. (r) drd. Eugen Valeriu POPA*

Securitatea cibernetică constituie o chestiune de interes şi importanţă globală; şi spaţiul cibernetic sau cyberspaţiul devenind noul domeniu al războiului. Potrivit Strategiei Canadei pentru Securitate Cibernetică (2010), spaţiul virtual înseamnă lumea electronică creată de reţelele interconectate de tehnologia informaţiei şi informaţiile cu privire la aceste reţele.

Pornind de la aceste aspecte, prezentul articol are ca obiectiv principal prezentarea unor aspecte privind politica de securitate cibernetică a Canadei, respectiv aspecte din Strategia Canadei pentru Securitate Cibernetică şi despre organizaţii canadiene cu atribuţii în domeniul securităţii cibernetice.

Cyber security is a matter of global interest and global importance; cyberspace has become the new field of war. According to Canada's Cyber Security Strategy (2010), cyberspace means the electronic world created by interconnected networks of information technology and intelligence on those networks.

Based on these aspects, this article aims at presenting the main aspects of cyber security policy of Canada, respectively aspects of Canada's Cyber Security Strategy and the Canadian organizations active in the field of cyber security.

Cuvinte-cheie: securitate cibernetică; Canada; strategie de securitate cibernetică; organizaţii; ameninţări.
Keywords*: cyber security; Canada; cyber security strategy; organizations; threats.*

Canada atrage un beneficiu din cooperarea cu Statele Unite ale Americii în spaţiul cibernetic, deoarece natura evoluţiei ameninţărilor şi costul combaterii acestor ameninţări sunt din ce în ce mai dificil de suportat pe cont propriu. Pe lângă cooperarea cu SUA şi cu alţi aliaţi apropiaţi, guvernul canadian se confruntă cu provocarea găsirii unui echilibru între securitatea cibernetică şi definiţia proprie a drepturilor şi a libertăţilor individuale. Astfel, reprezentanţii Camerei Comunelor din Parlamentul Canadei considerau, în luările de poziţie, că în perspectiva gestionării riscurilor cibernetice, datorită unei activităţi de cooperare mai intense între agenţiile guvernamentale care asigură securitatea cibernetică şi cele cu specific în intelligence, acestea pot avea puteri extinse pentru coordonarea contracarării atacurilor cibernetice împreună cu agenţiile americane şi cu alte agenţii aliate; în acelaşi timp, considerau că această sarcină nu trebuie lăsată la latitudinea agenţiilor specializate fără o supraveghere din partea reprezentanţilor politici.

Elementul de specificitate în domeniul securităţii cibernetice al Canadei este acela că, odată cu sporirea capacităţii tehnice şi operative pentru a face faţă ameninţărilor din spaţiul cibernetic, această ţară sporeşte şi capacitatea Camerei Comunelor de supraveghere a structurilor create şi ale acţiunilor principale ale acestora. Ideea înfiinţării unui Comitet constituit din reprezentanţi din tot spectrul politic, care să aibă avizul de securitate necesar şi capacitatea de a chema martori în cunoştinţă de cauză pentru a asigura echilibrul între activităţile care ţin de securitatea cibernetică şi valorile naţionale ale statului de drept privind drepturile şi libertăţile individuale, susţinută de către unii membri ai Partidului Liberal Canadian, se bucură de o largă susţinere şi în rândul celorlalte partide. Prin mecanismul unor verificări şi bilanţuri periodice, amănunţite şi eficiente asupra rolului şi activităţilor acestor agenţii, Parlamentul Canadian

Universitatea Naţională de Apărare „Carol I”
e-mail: *eugenvaleriu@gmail.com*

consideră că se poate realiza o îmbunătăţire semnificativă a securităţii şi a rezilienţei infrastructurilor cibernetice, în timp ce intruziunile în libertatea individuală pot fi reduse la minimum.

Alt aspect de specificitate al sistemului de securitate cibernetică al Canadei derivă din natura cooperării canadiano-americană în domeniul global al securităţii şi în particular al securităţii cibernetice.

Strategia pentru Securitate Cibernetică a Canadei

În anul 2010 au fost aprobate două strategii: „Strategia Naţională de Protecţie a Infrastructurii Critice” şi „Strategia Canadei pentru Securitate Cibernetică – Pentru o Canadă mai Puternică şi Prosperă”[1] având următoarele trei obiective:

- *securizarea sistemelor cibernetice guvernamentale şi a celor clasificate ca făcând parte din infrastructura critică*: acest obiectiv stabileşte roluri şi responsabilităţi clare, nu numai cu privire la asigurarea securităţii şi a rezilienţei sistemelor cibernetice guvernamentale, dar şi pentru sporirea nivelului de cultură de securitate cibernetică în cadrul sistemului public;
- *asigurarea sistemelor cibernetice care nu aparţin guvernului federal prin parteneriate public-private*: implicând atât actorii economici care exploatează infrastructuri critice, mediul privat, cât şi mediul academic de cercetare în domeniul securităţii cibernetice;
- *asigurarea suportului pentru dezvoltarea unei culturi de securitate şi securizare a mediului online pentru cetăţenii canadieni*: pentru reducerea infracţionalităţii cibernetice, protejarea cetăţenilor canadieni în mediul virtual şi confidenţialitatea datelor personale.

În concepţia Strategiei de Securitate Cibernetică a Canadei, capabilitatea de securitate cibernetică reprezintă atât puterea de a determina efectele operaţionale dorite într-o anumită zonă, cât şi menţinerea acestor efecte pe o perioadă determinată, aceasta fiind un efect combinat în care sistemele de intelligence de care dispune ajută la determinarea unor anumite efecte particulare.

În viziunea acestui document, capabilitatea de apărare cibernetică nu numai că se întinde dincolo de echipamente, infrastructuri şi sisteme software, ci mai degrabă include elemente de conexiune între aceste componente, care fac ca o capabilitate de apărare cibernetică să determine un efect operaţional precis. Aceste componente, care dau forma capabilităţilor, sunt descrise folosind algoritmul PRICIE, echivalentul american al DOTMLPF – Doctrină, Organizaţie, Pregătire, Material, Leadership şi Educaţie, Personal şi Facilitaţi (*Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities*)[2], care descompune capabilităţile în domenii de responsabilităţi funcţionale şi care se aliniază pe structura organizaţională astfel: Personal (*Personnel*), Cercetare/Dezvoltare (*Research & Development*), Infrastructură şi Organizaţie (*Infrastructure & Organization*), Concepte, Doctrine şi Instrucţie Colectivă (*Concepts, Doctrine & Collective Training*), Infrastructură de Comunicaţii şi IT (*IT&C Infrastructure*), Echipamente, Logistică şi Servicii (*Equipment, Logistics & Services*)[3].

Premergător elaborării acestei strategii, guvernul canadian a elaborat şi a implementat o serie de măsuri sectoriale care la momentul respectiv răspundeau punctual complexului de ameninţări din domeniul cibernetic. Dintre aceste măsuri amintim:

- În anul 2011, a fost lansat Serviciul Partajat Canadian (*Shared Services Canada – SSC)*[4], pentru a simplifica modul în care guvernul canadian gestionează sistemele federale de telecomunicaţii şi IT, centrele de date şi serviciile de e-mail; fiind gândit ca furnizor de servicii integrate ICT la nivelul întregii administraţii canadiene având ca scop optimizarea costurilor de implementare şi de operare a infrastructurii ICT guvernamentale şi aplicarea unei politici de securitate cibernetică eficientă pentru infrastructura ICT a întregului sistem de administraţie canadian. Tot în anul 2011, guvernul canadian a definit rolurile şi mandatele pentru Structura de Securitate a Comunicaţiilor Canadei (*Communications Security Establishment Canada – CSEC*)[5] şi pentru Centrul Canadian pentru Răspuns la Incidente Cibernetice (*Canadian Cyber Incident Response Centre – CCIRC*)[6], acestea fiind încorporate în Agenţia de Securitate Publică (*Public Safety Canada – PS*)[7], în scopul îmbunătăţirii capacităţii de identificare, prevenire şi gestionare a incidentele de securitate cibernetică. Ulterior, a fost lansat *GetCyberSafe*[8], un website creat de guvern în scopul de a creşte gradul de

conştientizare asupra ameninţărilor online şi de a informa cetăţenii canadieni despre problematica securităţii cibernetice, acesta fiind destinat în special părinţilor şi adolescenţilor fiind mai mult o colecţie de videoclipuri interactive şi informaţii despre hărţuirea cibernetică.

• În anul 2012, Canada a semnat un Planul de Acţiune pentru Securitatea Cibernetică (*Cyber Security Action Plan*)[9], în cadrul Planului de Acţiune Dincolo de Frontieră (*Beyond the Border Action Plan*)[10] iniţiat de Departamentul Apărării al Statelor Unite ale Americii, în scopul consolidării cooperării în probleme de securitate cibernetică între cele două ţări. Acest plan de acţiune iniţiat de către SUA în conformitate cu strategia de cooperare în domeniul securităţii cibernetice recunoaşte importanţa protejării infrastructurii critice digitale partajate între SUA şi Canada şi urmăreşte creşterea capacităţii de răspuns la incidente cibernetice. Prin semnarea acestui document, ambele state recunosc faptul că partajează infrastructuri critice care au o componentă cibernetică importantă şi faptul că disfuncţionalitatea unei componente, indiferent unde s-ar afla, afectează parametrii de funcţionare ai celorlalte. Tot în anul 2012, guvernul canadian a anunţat semnarea unui parteneriat public privat între Agenţia de Securitate Publică, în calitate de entitate guvernamentală şi STOP.THINK.CONNECT, o coaliţie de companii private din sectorul nonprofit şi organizaţii guvernamentale. Această coaliţie a fost creată la iniţiativa Departamentului Apărării al SUA şi a ajutat la alinierea campaniilor de conştientizare a publicului în Canada şi în SUA privind ameninţările cibernetice.

Organizaţii naţionale cu atribuţii în domeniul securităţii cibernetice

În continuare vor fi prezentate organizaţiile principale cu atribuţii în domeniul securităţii cibernetice din Canada, și anume:

• *Agenţia de Securitate Publică* este organizaţia mandatată să asigure securitatea cetăţenilor canadieni la o paletă largă de riscuri din categoria dezastrelor naturale, criminalităţii şi terorismului. Aceasta are în subordine Centrul Operaţional Guvernamental (*Government Operations Centre – GOC*)[11] ca şi hub pentru Sistemul National de Răspuns la Urgenţe (*National Emergency Response System – NERS*)[12]. În cazul unor incidente cibernetice majore care au impact semnificativ la nivel naţional, Centrul Canadian pentru Răspuns la Incidente Cibernetice (*Canadian Cyber Incident Response Centre* – CCIRC) redirecţionează către GOC managementul acestor incidente, iar coordonarea capabilităţilor de răspuns şi refacere va fi făcută de la nivelul NERS. Acest lucru permite o mobilizare rapidă a capacitaţilor de răspuns la incidente cibernetice majore atât al celor guvernamentale, din sectorul privat, dar şi activarea unor capacitaţi puse la dispoziţie de către DOD al SUA prin parteneriatele mai sus-menţionate.

• *Structura de Securitate a Comunicaţiilor Canadei* (CSEC) este agenţia de criptografie canadiană responsabilă cu analiza şi sinteza datelor criptografice şi cu cifrul Canadei; de asemenea, monitorizează şi apără reţelele guvernamentale canadiene prin detectarea, descoperirea şi răspunsul la ameninţările cibernetice complexe.

• *Poliţia Federală Canadiană* (RCMP) conduce şi efectuează investigaţiile judiciare la incidente cibernetice şi la alte acte penale care au ca şi componentă a acţiunii criminale tehnologia ICT. Aceasta are mandat de a conduce investigaţii penale în cazul unor incidente naţionale de securitate cibernetică şi de a asista partenerii interni şi internaţionali în ceea ce priveşte combaterea unor ameninţări cibernetice şi în acţiuni de combatere a utilizării sistemelor ICT de către grupurile de criminalitate organizată.

Serviciul de Informaţii şi Securitate Canadian (CSIS) efectuează investigaţii asupra riscurilor, ameninţărilor şi vulnerabilităţilor din spaţiul cibernetic care au impact direct asupra securităţii naţionale şi raportează guvernului canadian, la nivelul primului ministru, orice activitate care constituie o ameninţare la securitatea Canadei. CSIS este responsabil de elaborarea de analize şi sinteze pentru guvernul canadian privind ameninţările cibernetice, intenţiile şi capabilităţile actorilor din spaţiu cibernetic care operează intern şi extern şi care reprezintă o ameninţare la adresa securităţii statului canadian şi al intereselor sale. Această structură guvernamentală este mandatată de guvernul federal să ia măsurile destinate a preveni şi a combate spionajul cibernetic şi orice altă ameninţare din domeniul cibernetic la adresa infrastructurilor critice ale Canadei.

Departamentul Apărării Naţionale al Canadei (DND) este structura responsabilă cu asigurarea capabilităţilor de apărare şi intelligence pentru

apărarea cibernetică; contribuie la managementul incidentelor cibernetice prin utilizarea capabilităţilor cibernetice proprii şi ale aliaţilor săi în procesul de monitorizare şi de analiză a incidentelor cibernetice majore de către NERS. De asemenea, asistă cabinetul prim-ministrului pentru analiza opţiunilor pentru un potenţial răspuns militar la agresiunile din spaţiul cibernetic şi acţionează în calitate de legătură între guvernul canadian şi aliaţii săi militari.

Centrul Canadian Anti-Fraudă (CAFC) este depozitarul central pentru date, informaţii şi resurse materiale referitoare la fraude; furnizează către partenerii guvernamentali, companiile comerciale şi cetăţenii canadieni în timp util informaţii precise şi utile în sprijinul aplicării legislaţiei economice canadiene.

federal şi componentele sale de răspuns şi recuperare la incidentele cibernetice va fi prin intermediul CCIRC. Ca parte a Agenţiei de Securitate Publică, CCIRC a stabilit relaţii de lucru la nivel federal cu alte agenţii federale. Fluxul de raportare al unui incident cibernetic cu consecinţe noncibernetice este prezentat în figura nr. 1[13], fiind organizat pe trei nivele logice; decizia şi urmărirea procesului de escaladare fiind în responsabilitatea CCIRC.

CCIRC este membru al Forumul International al Echipelor de Răspuns la Incidente de Securitate Cibernetică (*Forum of Incident Response and Security Teams* – FIRST)[14] încă din anul 2003; în prezent operează cu 12 echipe[15] şi colaborează direct cu: Centrul de Răspuns la Incidente de Securitate Cibernetică al USA – US-CERT[16], Centrul de Răspuns la Incidente de Securitate Cibernetică

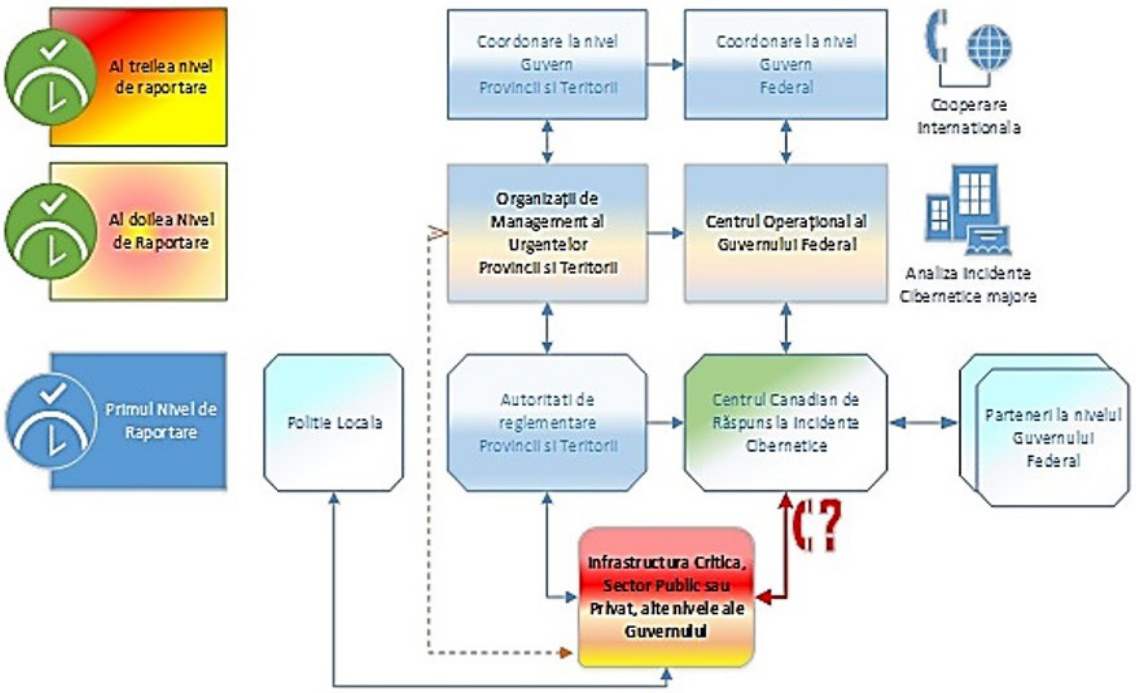

Fig. 1 *Fluxul de raportare al unui incident cibernetic cu consecinţe noncibernetice*

De asemenea, există numeroase departamente guvernamentale federale care joacă un rol activ în coordonarea unui răspuns la incidentele informatice, însă din punct de vedere operativ coordonarea acestora se realizează în cele mai multe cazuri prin intermediul CCIRC, acesta fiind centru naţional de coordonare pentru prevenirea, răspunsul şi recuperarea pentru incidentele cibernetice. În cele mai multe cazuri, primul contact pe care o organizaţie afectată o are cu structurile guvernului

al Regatului Unit al Marii Britanii – CERT-UK[17], Centrul de Răspuns la Incidente de Securitate Cibernetică al Australiei – CERT Australia[18]. De asemenea, CCIRC colaborează în mod direct şi cu Capabilitatea de Răspuns la Incidente Cibernetice a NATO (*NATO Computer Incident Response Capability* – NATO N-CIRC)[19] pentru prevenirea şi combaterea incidentelor cibernetice majore.

Din punctul de vedere al guvernului canadian şi al societăţii canadiene în ansamblu ei, securitatea

cibernetică este mai mult decât o problema tehnică, fiind privită ca fiind securitatea unui întreg ecosistem de comunicaţii, acesta fiind suportul pentru schimbul de informaţii publice şi private, pentru comunicare şi relaţii sociale. Securitatea cibernetică nu este definită de către strategii canadieni ca un scop în sine, ci ca o utilitate sau necesitate, acesta fiind şi punctul de vedere al economistului politic canadian Robert Cocs, care afirma: „…Există mai multe moduri diferite de a asigura spaţiul virtual, în funcţie de preferinţele politice şi valorile la ceea ce trebuie să fie protejate în primul rând. Securitatea cibernetică este, prin urmare, în mod inerent o discuţie despre filosofie politică”[20].

Concluzii

Dezvoltarea securităţii cibernetice în Canada este strâns legată de poziţia sa geostrategică şi geopolitică care o plasează în materie de securitate şi apărare cibernetică în spaţiul de influenţă nord-american. Această legătură a determinat, în ultimul deceniu, evoluţia politicilor de apărare şi securitate naţională ale Canadei, precum şi dezvoltarea ulterioară a infrastructurii de securitate cibernetică naţională a ţării. Semnificaţia acestei legături este explicată prin faptul că dezvoltarea securităţii naţionale cibernetice este în mare măsură determinată de nivelul de importanţă pe care guvernul federal canadian o acordă securităţii naţionale şi internaţionale; acesta din urmă fiind influenţat de nivelul şi forma relaţiilor sale cu vecinul său important, SUA. Deşi de-a lungul timpului, relaţiile de colaborare SUA-Canada în ceea ce priveşte securitatea cibernetică s-au calificat, în general, ca excepţionale, acestea au fost, totuşi, marcate de tensiuni, în special în ceea ce priveşte abordarea în timpul operaţiilor cibernetice comune a diferenţelor privind drepturile şi libertăţile individuale versus nevoia de securitate sau metodele şi mijloacele utilizate în îndeplinirea acestor misiuni comune, ceea ce face din Canada un critic obişnuit al SUA relativ la operaţiile de spionaj cibernetic.

Influenţa istorică a Marii Britanii, fosta patrie mamă şi unul dintre cei mai importanţi actori economici şi militari globali, a cărei contribuţie istorică la menţinerea suveranităţii Canadei, este recunoscută de strategii canadieni prin păstrarea unor relaţii privilegiate şi în domeniul asigurării securităţii cibernetice[21].

Din punct de vedere politic, sosirea unui guvern majoritar federal în anul 2015, condus de către liberalul Justin Trudeau şi recunoaşterea vulnerabilităţii Canadei în ceea ce priveşte securitatea cibernetică din cauza lipsei unei industrii autohtone care să ofere componenta de rezilienţă a infrastructurii canadiene de apărare cibernetică, în următorii ani va accelera cel mai probabil procesul de sprijin al cercetării şi al dezvoltării în domeniu, chiar şi la nivel federal.

Strategia de securitate cibernetică a Canadei păstrează caracterul acesteia de ţară democratică liberală. Din perspectiva acestei strategii, spaţiul cibernetic este un ecosistem deschis şi distribuit şi este privit ca o resursă comună mixtă în care însă cea mai mare parte este gestionată de sectorul privat. Documentele strategice din domeniu păstrează principiile şi măsurile de protecţie ale drepturilor şi libertăţilor individuale înscrise în Constituţia acestei ţări.

NOTE:

1 *Canada's Cyber Security Strategy*, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx, accesat la 10.05.2016.

2 Department of the Army Headquarters, United States, Army Training and Doctrine Command Fort Eustis, Tradoc Regulation 71-20, *Concept development, capabilities determination, and capabilities integration*, https://acc.dau.mil/.../TRADOC%20Concept%20Development, accesat la 28 iunie 2013.

3 Clive Kerr, Robert Phaal, David Probert, *A Framework For Strategic Military Capabilities În Defense Transformation*, 11th International Command and Control Research and Technology Symposium Coalition Command and Control in the Networked Era, Cambridge 26-28 Septembrie 2006, http://www.dodccrp.org/events/11th_ICCRTS/html/papers/061.pdf, accesat la 10.05.2016.

4 http://www.ssc-spc.gc.ca/index-eng.html, accesat la 10.05.2016.

5 https://www.cse-cst.gc.ca/en, accesat la 10.05.2016.

6 http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cc irc-ccric-en.aspx, accesat la 10.05.2016.

7 http://www.publicsafety.gc.ca/index-eng.aspx, accesat la 10.05.2016.

8 http://www.getcybersafe.gc.ca/index-eng.aspx, accesat la 10.05.2016.

9 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx, accesat la 10.05.2016.

10 https://www.dhs.gov/action-plan, accesat la 10.05.2016.

11 http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr-en.aspx, accesat la 10.05.2016.

12 http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-rspns-sstm/index-eng.aspx, accesat la 10.05.2016.

13 https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx, accesat la 10.05.2016.

14 https://www.first.org/about/mission, accesat la 10.05.2016.

15 https://www.first.org/members/map#canada, accesat la 10.05.2016.

16 https://www.us-cert.gov/, accesat la 10.05.2016.

17 https://www.cert.gov.uk/, accesat la 10.05.2016.

18 https://www.cert.gov.au/, accesat la 10.05.2016.

19 http://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 10.05.2016.

20 Robert W. Cox, *Social Forces, States and World Orders: Beyond International Relations Theory*, https://ic.ucsc.edu/~rlipsch/Pol272/Cox.pdf, accesat la 14.05.2016.

21 Benoit Gagnon, *Informatique et cyberterrorisme*, http://www.cicc.umontreal.ca/ files/prod/publication_files/annuaire_2009_2010-final.pdf, accesat la 14.05.2016.

BIBLIOGRAFIE

*** *Canada's Cyber Security Strategy For a stronger and more prosperous Canada*, 2010.

*** *Action Plan 2010-2015 for Canada's Cyber Security Strategy*, 2013.

Moens Alexander, Cushing Seychelle, Dow W. Alan, *Cybersecurity challenges for Canada and the United States*, martie 2015.

http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

https://acc.dau.mil/.../TRADOC%20Concept%20Development

http://www.dodccrp.org/events/11th_ICCRTS/html/papers/061.pdf

http://www.ssc-spc.gc.ca/index-eng.html

https://www.cse-cst.gc.ca/en

http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

http://www.publicsafety.gc.ca/index-eng.aspx

http://www.getcybersafe.gc.ca/index-eng.aspx

http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx

https://www.dhs.gov/action-plan

http://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr-en.aspx

http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-rspns-sstm/index-eng.aspx

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx

https://www.first.org/about/mission

https://www.first.org/members/map#canada

https://www.us-cert.gov/

https://www.cert.gov.uk/

https://www.cert.gov.au/

http://www.nato.int/cps/en/natohq/topics_78170.htm

https://ic.ucsc.edu/~rlipsch/Pol272/Cox.pdf

http://www.cicc.umontreal.ca/files/prod/publication_files/annuaire_2009_2010-final.pdf

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

https://www.fraserinstitute.org/sites/default/files/cybersecurity-challenges-for-canada-and-the-united-states.pdf