Crown in the clouds: a Canadian data sovereignty crisis

Neal Kushwaha
Founder and CEO, Impendo Inc.
Ottawa, Canada
neal@impendo.com

Bruce W. Watson
Chief Scientist, IP Blox
Eindhoven, Netherlands
bruce@ip-blox.com

Abstract: Cloud Service Providers (CSP) offer the opportunity for individuals, companies, and governments to rapidly leverage current capabilities dynamically and with great elasticity. At the time of writing, unlike the U.S., Canada does not have large sovereign CSPs with global presence.

Although one may debate overall cost effectiveness and value of moving electronic data and computational workloads to the cloud, it is difficult to ignore the international drive for the adoption of cloud and cloud services. The Government of Canada's (GC) use of cloud capacities should not be driven by technical and economic desires or requirements. Like decision making in warfare, the complexities of international law and politics should be considered.

This paper reflects upon the lessons learned from the U.S. "Cloud First" policy and discusses the challenges and risks of hosting sovereign Canadian electronic data and workloads in the cloud, concluding that is unclear if the GC will be able to claim data sovereignty even if its data is stored in Canada using a global CSP.

Keywords: *cloud, data sovereignty, international law, Government of Canada*

1. INTRODUCTION

The Government of Canada (GC) maintains electronic data and computational workloads that are categorised with security designations named "unclassified", "protected" (expected to cause varying degrees of injury to a non-national interest), and "classified' (expected to cause varying degrees of injury to the national interest).

Outsourcing electronic data storage and computational workloads to public companies, known as Cloud Service Providers (CSP), in a public, hybrid, and private cloud has become a matter of importance to the Canadian Federal Government.

In November 2017, the GC Treasury Board of Canada Secretariat (TBS) released the "Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021" as an update to the "Government of Canada Information Technology Strategic Plan 2016-2020". Of the six guiding principles described in the 2017-2021 IM/IT strategic plan, guiding principle 5, "Cloud first approach", states (Treasury Board of Canada Secretariat 2017):

> *Departments will explore "… as a service" (XaaS) cloud services before developing solutions in-house. This includes private and public cloud offerings".*

Of the 75 strategic actions detailed within the same document, guiding principle 5 specifies the following four:

- Strategic action 7: Adopt cloud services;
- Strategic action 8: Establish a cloud service broker;
- Strategic action 9: Offer public cloud services; and
- Strategic action 10: Offer private cloud services.

These four strategic actions have been remapped into the current GC strategic plan, "Digital Operations Strategic Plan: 2018-2022" under Chapter 4, strategic action #16 "Workload migration and cloud adoption" (Treasury Board of Canada Secretariat 2019). These strategic actions are intended to survive until 2023.

Shared Services Canada (SSC) recently signed two contracts with CSPs[1], specifically Amazon Web Services (AWS) Canada and Microsoft Canada Azure services for up to protected B category of information. SSC acts as a broker for any GC department's cloud services but is not accountable to them for their security of information being hosted. SSC has arrangements[2] with 23 suppliers (also known as resellers) and 8 providers offering a range of infrastructure (IaaS), software (SaaS), and platform (PaaS)as a service, namely:

1. AWS Canada Inc., headquartered in the U.S. offering IaaS, SaaS, and PaaS;
2. Google Canada Corp., headquartered in the U.S. with unconfirmed offerings;
3. IBM Canada Ltd, headquartered in the U.S. offering SaaS and PaaS;
4. Microsoft Canada Inc., headquartered in the U.S. offering IaaS, SaaS, and PaaS;
5. Oracle Corp Canada Inc., headquartered in the U.S. with unconfirmed offerings;
6. OVH Canada, headquartered in France offering IaaS;
7. Salesforce.com Canada Corp, headquartered in the U.S. offering SaaS; and
8. ThinkOn Inc., headquartered in Canada offering IaaS and PaaS.

In a whitepaper published June 17, 2019 (Treasury Board of Canada Secretariat 2019), TBS discusses data sovereignty as it relates to public cloud services. In consultation with SSC, Public Services and Procurement Services Canada, and Communications Security Establishment Canada (CSE, Canada's cryptologic and signal intelligence agency), various technological data requirements are described, but matters of international law and political concerns are not. The whitepaper touches on "data residency" and "data sovereignty" but does not consider the challenges described herein.

2. U.S. "CLOUD FIRST" POLICY

In December 2010 the then CIO of the U.S. Government published a "25 Point Implementation Plan to Reform Federal Information Technology Management" and began advocating a "Cloud First Policy". One of the goals was to have each federal agency move three services to the cloud within 18 months. Below are actions 3 and 4 of the 25 actions (Kundra 2010, pp 6-8).

[1] SSC Tweets: "*Our exciting journey to the Cloud continues with the signing of the first two contracts for Protected B services.*" (Shared Services Canada 2019).

[2] SSC's website to help understand its GC cloud broker responsibility (Shared Services Canada 2019).

- *Action 3: Shift to "Cloud First" policy. Each agency will identify three "must move" services within three months, and move one of those services to the cloud within 12 month and the remaining two within 18 months*
- *Action 4: Stand-up contract vehicles for secure IaaS solutions. Within the next six months, after completing security certification, GSA will make a common set of contract vehicles for cloud-based Infrastructure-as-a-Service solutions available government-wide.*

Later, the U.S. Government Accountability Office (GAO) published a study titled "Cloud Computing: Additional Opportunities and Savings Need to Be Pursued" describing the progress of seven agencies and the benefits thus far gained, comparing July 2012 to July 2014 quantitative results. The seven agencies are as follows (U.S. Government Accountability Office 2014, pp 11-15):

1. Agriculture;
2. General Services Administration (GSA);
3. Health and Human Services (HHS);
4. Homeland Security (DHS);
5. Small Business Administration (SBA);
6. State; and
7. Treasury.

As of July 2012, the seven agencies added a total of 21 new services to the cloud as expected. By July 2014, the same agencies added a total of 80 more, for a total of 101. The report also states the varying number of implemented services by department, noting that the Treasury, SBA, and DHS had implemented only 2, 3, and 5 respectively while HHS, GSA, and State had implemented 33, 18, and 11 respectively between the two study dates of July 2012 and July 2014.

Out of a total of 2000 potential services, 245 (12%) were evaluated and selected for cloud services, 410 (21%) were evaluated but not selected for cloud services, while 1345 (67%) were not selected for evaluation at all.

The reason why so many services were not evaluated for cloud services cited by the agencies was that they were all legacy systems and that a cloud solution would only be considered for these legacy systems upon their modernization or end-of-life.

The document highlights the challenges these U.S. agencies faced in terms of managing legacy systems. The GC faces a similar challenge. Much of the GC is operating legacy systems that would not be suitable for cloud services, a complexity discovered in their workload-migration efforts. Furthermore, the procurement model of the GC will need to align with the ability to take advantage of the elasticity of the cloud services versus paying for maintaining availability.

Economic viability

The GAO also noted the increase in actual spend versus budgeted values. The seven agencies in the report increased their spending by $222 million USD for a total $529 million USD. The total $529 million USD represents only 2.45% of the $21.3 billion USD budget of these seven agencies.

The U.S. has large buying power and in 2013 the Central Intelligence Agency (CIA) awarded Amazon a $600 million USD 10-year contract, which IBM challenged in court as their price was lower. Then Amazon countered with their case, stating the CIA should be able to go with who they choose. This shaky start to the classified cloud service resulted in a U.S. Intelligence multi-agency use system through Amazon's existing Commercial Cloud Services (C2S) which today exceeds the $600 million USD contract issued by

the CIA. It should be noted, (1) the CIA's entire requested 2013 budget (leaked in 2013[3]) was $14.7 billion USD and (2) this contract likely does not cover 100% of the CIA's information technology budget. The 10-year $600 million USD contract represents just slightly less than 0.41% of the CIA's entire annual budget (at the time of contract award).

In comparison with Canada, the entire expenditures of the Canadian Security Intelligence Service (Canada's human intelligence service) for fiscal year 2017/2018 was $587.0 million CAD (Treasury Board of Canada Secretariat 2019, p I-7). Assigning 0.41% of this budget to a cloud solution would result in $24.0 million CAD for a similar 10-year period, or equally distributed at $2.4 million CAD annually over 10 years.

For Canada to benefit from a similar contract in the U.S., a multi-department agreement with CSPs will likely need to be drafted, consisting of various departments with similar intentions, risk tolerances, and level of classified information.

3. NOTABLE CASES OF DATA EXPOSURE

Aside from the challenges described above, using cloud services present other challenges. In 2017, the following four cases were publicized by the media whereby U.S. Government classified data on Amazon private cloud services were exposed to the public.

1. May 24, 2017: 28 gigabytes (over 60,000 files) of Pentagon and National Geospatial Intelligence Agency classified intelligence data tied to military projects that contained unencrypted passwords and security credentials belonging to government contractors with active Top Secret security clearance were exposed on Amazon servers (Ashok 2017).
2. Sep 4, 2017: 9,402 files containing details of U.S. Intelligence operatives with Top Secret clearance were exposed on Amazon Simple Storage Service (S3) servers. All files were exposed in a folder titled "*resumes*" which included the CVs of U.S. Department of Defense and U.S. intelligence community members (O'Sullivan, Insecure: How A Private Military Contractor's Hiring Files Leaked 2019).
3. Sep 6, 2017: Three Amazon S3 buckets containing over 1.8 billion scraped internet posts and news comments over an 8 year period (2009-2017) from various countries by U.S. CENTCOM and PACOM. The breach highlighted the use of the U.S. Army's Coral Reef software. Although the information available indicated countries of the Middle East and Asia, the content included comments from the official Facebook page of todays' Pakistani Prime Minister, Imran KHAN (O'Sullivan, Dark Cloud: Inside The Pentagon's Leaked Internet Surveillance Archive 2019).
4. Sep 27, 2017: NSA and U.S. Army files from an AWS domain labelled U.S. INSCOM were configured for public access. The files, including an Oracle Virtual Appliance (OVA) which when loaded into VirtualBox, revealed multiple virtual partitions (between 1 GB and 69 GB in size), contained files marked as Top Secret//NOFORN, private keys for accessing other distributed systems, and hashed passwords. The exposed data included 8 sub-programs. The OVA disk image anticipated use was to be deployed in the field for collecting intelligence data. It appeared to connect to Pentagon systems to submit intelligence data (O'Sullivan, Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online 2019).

[3] "*Spending by the CIA has surged past that of every other spy agency, with $14.7 billion in requested funding for 2013*" (Gellman and Miller 2013).

Although there is much dispute as to how this information was made available or divulged, in the end, the information was made public and it impacted the respective departments'/agencies' reputations, some individuals, and exposed U.S. intelligence gathering methods, which cannot be undone. The entire repositories were available for download.

Another challenge such breaches bring to light are political. Certain breaches expose the methods and/or targets that can limit the government's ability to negotiate or offer evidence to another nation to possibly claim breach of sovereignty under international law.

4. STORING GC DATA OUTSIDE OF CANADA

In May of 2017, SSC's then Assistant Deputy Minister of Cyber and IT Security branch wrote a memorandum to SSC's Chief Operating Officer regarding storing data on 3rd party cloud services that are hosted outside of Canada. Even if Canada uses their own cryptographic keys as "Bring Your Own Key", CSE does not consider it adequate for hosting classified data in the cloud in cases of "data in use".[4]

CSE advised SSC further that using "Hold Your Own Key" introduces a layer of complexity that tends to impact availability of the data. It only applies to data at rest, not data in use. Microsoft has described how only a few of their clients use this model.

Finally, SSC and CSE were advised that if the U.S. Government presents a legal request to data, Microsoft would inform their clients prior to releasing the data.

While such discussions were underway in Canada, the governments of Estonia and Luxembourg were negotiating the final details of their mutual agreement which would deliver the world's first data embassy. Today, the Betzdorf data centre behaves as a sovereign Estonian embassy that hosts the nation's "*most critical and confidential data*"[5], prohibiting Luxembourg from accessing the data.

Completely opposite to the Canadian thoughts, Estonia set out to not just host their data in a foreign state, but also ensure all their nation's citizens and governments would be able to securely authenticate and login to critical services in the event of another national cyber-conflict.

The entire solution for Estonia may not be considered cost-effective, but it serves as a backup of their data and services delivering protections from their bordering neighbour's threats and risks, like the Russian based cyber-offensive the nation of Estonia suffered in 2007.

5. USING CLOUD SERVICE PROVIDERS WITHIN CANADA

Between 2013 and 2018, there were cases between Microsoft and the U.S. Department of Justice (DOJ) regarding a very specific warrant under the Stored Communications Act (SCA) of the Electronic Communications Privacy Act (ECPA) of 1986. Microsoft's data centre in Dublin, Ireland held email data that was of interest to the U.S. Government. The U.S. DOJ argued that if the data can be accessed "*domestically with the click of a computer mouse*", then the U.S. ECPA of 1986 can be applied to access

[4] An Access to Information request filed by Dean Beeby of CBC News resulted in the release of an SSC briefing note (Thuppal and Mohan 2017), https://www.cbc.ca/news/politics/storage-data-cloud-government-canadian-shared-services-microsoft-secret-1.4277836.

[5] Quote by Siim Sikkut, Estonia's ICT policy adviser "*The Luxembourg site will store the copies of the most critical and confidential data*" (e-Estonia Briefing Centre 2017).

the data (United States of America, petitioner v. Microsoft Corporation, Petition for a writ of certiorari 2017, p 12).

The court documents filed by the U.S. DOJ do not specify if the intended target of the emails they were attempting to access were those of a U.S. citizen or a foreigner. It does state that the U.S. DOJ believed the user's email account was being used to conduct criminal drug activity. Had the U.S. Supreme Court sided with the DOJ on this matter, it would have set a precedence for data stored in the cloud and how data (including personal, commercial, and national) is perceived as secure.

While the case was under appeal at the U.S. Supreme Court, on March 23, 2018, U.S. President Trump signed the Clarifying Lawful Overseas Use of Data (CLOUD) Act into law. The U.S. CLOUD Act contains two parts. Part 1 added a new subsection within the Wiretap Act (title 18 U.S.C. § 2523) and amended other sections within both the Wiretap Act and Stored Communications Act, while part 2 added a new subsection within the Stored Communications Act (title 18 U.S.C. § 2713).

The first part (title 18 U.S.C. § 2523) allows for the U.S. to enter into executive agreements with other nations that meet a specific set of criteria including adhering to the Convention on Cybercrime (also known as the Budapest Convention). These executive agreements allow the U.S. to permit U.S. based global CSPs to respond and provide foreign law enforcement agencies with evidence stored within their company's information and communications technology (ICT) in any country, thereby avoiding any conflicts with other 3rd party nation's laws. Currently, only the U.K. has entered into such an agreement with the U.S (U.S. Department of Justice 2019).

When the U.S. enter into executive agreements with other nations, it does not imply that the foreign nation has any jurisdiction over a particular U.S. based global CSP nor does the U.S. require the other nation's CSPs to comply with any requests for evidence by the government of the U.S.

The second part of the act allows for extraterritorial reach of all U.S. company data (title 18 U.S.C. §2713):

> *Required preservation and disclosure of communications and records: A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.*

This latter part of this act, while under appeal at the U.S. Supreme Court, mooted the case of U.S. v. Microsoft Corporation (United States of America v. Microsoft Corporation 2018).

Large U.S. CSPs such as Microsoft Corporation and Amazon Web Services Inc. commonly operate and offer their services in Canada under a Canadian corporation. Both Microsoft Canada Inc. and Amazon Web Services Canada Inc. offer their Canadian customers the option to host their data in Canadian data centres. Although a Canadian citizen, corporation, or the GC may consider this adequate, with the enacting into law of the U.S. CLOUD Act, these Canadian entities may not only be exposing their data to various U.S. law enforcement agencies, but also to the unknown 3rd party nations holding executive agreements with the U.S.

In line with the U.S. CLOUD Act, the proposed EU e-evidence regulation (COM/2018/225 final) allows for the extraterritorial reach along with preservation and production of data, stored by a service provider in another jurisdiction, necessary as evidence in criminal investigations.

> *By introducing European Production Orders and European Preservation Orders, the proposal makes it easier to secure and gather electronic evidence for criminal proceedings stored or held by service providers in another jurisdiction.*

Under the proposal, member states will be required to respond to requests within 10 days for standard requests. In cases of emergency, the response time is 6 hours. The response times are significantly reduced compared to the existing 120 days for European Investigation Orders and 10 months for Mutual Legal Assistance. The proposal described four data types that are covered under the Production Orders and Preservation Orders.

1. Subscriber data: personal information used to identify an individual, commonly considered PROTECTED B information at the GC, including name, address, billing information, date of birth, email address, telephone number, etc.
2. Access data: a component of metadata, including the logon and log-off date and times, IP addresses assigned by service providers, etc.
3. Transactional data: a component of metadata, including geolocation of the source and destination of the data, size of data, route, the communication protocol, etc.
4. Content data: the digital data being consumed by the user in voice, video, audio, text, images, etc.

Both Orders are only applicable to criminal offences carrying a punishable sentence of 3 years or more (or specific cybercrimes and terrorism crimes) in the issuing nation state. Responding to all Production Orders with electronic evidence is mandatory by each service provider and must meet General Data Protection Regulation. The proposal applies to any service provider, regardless of where the parent company is located or where the data is held.

6. SOVEREIGNTY

The discussion of the applicability of nation state laws brings into question the interpretation of international law by various states. In order to violate sovereignty over cyber, one would need to violate territorial integrity or impact inherently governmental functions.

Chapter "Cyber Warfare" of Solis' textbook (Solis 2016, pp 680-681) and Tallinn Manual 2.0 rule 92 (Schmitt and Vihul 2017, p 415) both define a cyber attack as "*a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.*"

As an example, close access cyber operations of any kind resulting in functional damage would likely violate territorial integrity. Cyber actions causing permanent physical damage to ICT infrastructure or permanently encrypting all data (including any backups) also would likely violate sovereignty. The mystery lies in temporary violations, such as those causing slowdowns, port scanning, performing espionage by remotely operating within ICT and copying data, or sabotage by implanting malware for future use that may be destructive.

In response to breaches of sovereignty through cyber means, nation states may perform countermeasures, apply pleas of necessity, use retorsion, or claim self-defence. For self-defence, the U.S. position remains that any use of force is an armed attack, most likely including those over cyber.

U.S. (2012 and 2016)

During a question and answer period at the USCYBERCOM Inter-Agency Legal conference held on September 18, 2012, regarding a question related to state sovereignty in cyberspace, the former U.S. State Department's legal advisor Harold Koh stated (Koh 2012, Answer 9):

> *"Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered."*

Later, in his speech on November 10, 2016 regarding International Law and Stability in Cyberspace at the Berkeley Law School, Brian Egan expanded on Koh's response by stating (Egan 2017, p 174):

> *"…remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or de minimis effects.*"

The statements describe the importance the U.S. places on sovereignty while allowing for cyber espionage, indicating that violations of either territorial integrity or inherently governmental functions is considered unlawful in cyberspace.

U.K. (2018)

The U.K.'s position on cyber sovereignty is not the same as the U.S. On May 23, 2018 at Chatham House, the former U.K. Attorney General Jeremy Wright delivered a speech on international law and cyberspace where he stated (Wright 2018):

> *"Some have sought to argue for the existence of a cyber specific rule of a 'violation of territorial sovereignty' in relation to interference in the computer networks of another state without its consent.*
>
> *Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law."*

The U.K. position is that cyber sovereignty is not a rule that can be violated. If so, then it likely allows for other nation states to perform cyber operations upon the U.K. without violating the U.K.'s sovereignty. Furthermore, the U.K. cannot respond with countermeasures claiming state responsibility, because their cyber sovereignty cannot be violated.

Estonia (2019)

During her keynote on May 29, 2019 at CyCon, President Kersti Kaljulaid affirmed Estonia's position stating "*existing international law applies in cyber space"* while noting certain grey areas still exist. Though the President's position on sovereignty being a rule that can be violated by cyber was lacking, she did state (Kaljulaid 2019):

> *"Sovereignty entails not only rights, but also obligations. States are responsible for their internationally wrongful cyber operations just as they would be responsible for any other activity based on international treaties or customary international law. This is the case whether or not such acts are carried out by state organs or by non-state actors supported or controlled by the state. States cannot waive their responsibility by carrying out malicious cyber operations via non-state actors. If a cyber operation violates international law, this needs to be called out."*

France (2019)

France has taken a very strict position siding with the rule of cyber sovereignty. The document released by le ministère des Armées de la France on September 2, 2019, states (Ministère des Armées 2019, p13):

> *« Contrairement à la définition adoptée par les experts du Manuel de Tallinn, la France ne retient pas uniquement l'existence de critères matériels pour qualifier une cyberopération d'attaque. En effet, elle considère qu'une cyberopération constitue une attaque dès lors que les équipements ou les systèmes visés ne rendent plus le service pour lesquels ils ont été mis en place, que cela soit de manière temporaire ou définitive, réversible ou non. Dans le cas d'effets temporaires et/ou réversibles, l'attaque est caractérisée dès lors qu'une intervention de l'adversaire est nécessaire pour rendre l'infrastructure ou le système de nouveau opérant (réparation des équipements, remplacement d'une pièce, réinstallation du réseau, etc.). »*

> *« Contrairement au Manuel de Tallinn, la France considère qu'une attaque au sens de l'article 49 du PA I peut être caractérisée en l'absence de blessures ou de pertes humaines, ou de dommages physiques à l'encontre de biens. Ainsi, une cyberopération constitue une attaque si les équipements ou les systèmes visés ne rendent plus le service pour lesquels ils ont été mis en place, ceci y compris de manière temporaire et réversible, dès lors qu'une intervention de l'adversaire est nécessaire pour rendre l'infrastructure ou le système de nouveau opérant. »*

In both cases above, France rejected and clarified the Tallinn Manual 2.0 definition of a cyber attack claiming:

1. temporary effects or annoyances (example distributed denial of service) can also be interpreted as attacks and violations of sovereignty; and
2. cyber attacks, including those which do not cause physical injury or death to persons or damage or destruction to objects, are considered an attack under Article 49 Additional Protocol I of the Geneva Convention.

This essentially means, any cyber operation, including penetration or espionage, that impacts French ICT or territory as a result of a cyber operation may represent a violation of French sovereignty.

UN Group of Governmental Experts (GGE)

In June of 2013, appointed experts from 15 states (including Canada), reached a consensus on the UN GGE report (UN Doc. A/68/98) "Developments in the field of ICT in the context of International Security". The report's paragraph 20 reads as follows.

> *20. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.*

Over 2 years later, in July of 2015, a new appointed group of 20 experts (not including Canada), reached a consensus on the continuation the UN GGE study and report (UN Doc. A/70/174). Notably, the report's paragraphs 26, 27, and 28(b) under "How International Law applies to the use of ICTs" reads as follows.

> *26. In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; …*
>
> *27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.*
>
> *28. … the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States:*
>
> *(b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;*

Both UN GGE reports of 2013 and 2015 confirm that sovereignty applies to ICT in cyber space. However, if Canada were to store their sovereign data on another nation's ICT, for example the U.S., their data sovereignty may not be as clear. Canada will likely need to request their U.S. ally to assist in any breach of the ICT by a malicious state and will likely not be lawfully able to perform any form of response to breach of sovereignty, as Canadian ICT sovereignty will not have been breached.

The U.S., U.K. and France have taken clear positions regarding cyber sovereignty while Estonia and the Netherlands (Bijleveld 2018) remain less clear. Nevertheless, we must wait to see how the International Court of Justice and other nation states interpret the law for such cases.

7. CONCLUSION

CSPs are ever-changing, offering new capabilities and features. Maintaining a constant level of security requires more than reviewing and processing technological changes. The legal and political changes should not be neglected.

With the U.S. CLOUD Act and the proposed EU e-evidence regulation (COM/2018/225), the GC should remain cautious when proceeding to use CSPs that are headquartered in foreign states.

Foreign CSPs looking to maintain good standing with their respective governments and laws, may consider keeping active copies of their customer's data and respective metadata in their headquarter country. For CSPs offering services to the EU, having to comply with an emergency Production Order in 6 hours may not be possible without duplication and active parsing of customer data in a central location.

Using public, hybrid, and private capabilities within the GC:

1. will not necessarily result in cost effective or affordable solutions;
2. will likely require regular security reviews of CSP offering changes (especially for native cloud solutions);

3. will likely increase the risk to information exposure to other deliberate international actors and thereby impacting domestic and foreign reputation;
4. will likely require a constant pulse on legal positions and active cases of nation states; and
5. will likely require briefings to and inputs from the Prime Minister's Office of Canada for political reasons.

Consider the following scenario.

1. State A (Canada) stores data in the cloud on ICTs located in:
    a. State A and possibly duplicated to State B (U.S. or France) ICT; and
    b. State B ICT.
2. State C conducts cyber operations and exfiltrates State A's data located on ICT in State B.

Contemplate the political and domestic legal challenges that may arise if Canadian citizen or corporate data is breached due to the GC consciously storing their information in another nation state.

One may claim policy and technical reasons that GC data may never be hosted in another nation state, however, it is already doing so under several GC departments. In the scenario and at this time, it is unclear if the GC will be able to claim data sovereignty when State B ICT is breached.

REFERENCES

Ashok, India. 2017. "Pentagon leak: 28GB intelligence data was freely exposed on Amazon server by Booz Allen Hamilton." *International Business Times.* 1 Jun. https://www.ibtimes.co.uk/pentagon-leak-28gb-intelligence-data-was-freely-exposed-amazon-server-by-booz-allen-hamilton-1624236.

Bijleveld, Ank. 2018. "Keynote HE Ms. Ank Bijleveld MA, Minister of Defence." *Netherlands Military Law Review, Ministerie van Defensie.* 17 Aug. https://puc.overheid.nl/mrt/doc/PUC_248478_11/.

e-Estonia Briefing Centre. 2017. "Estonia to open the world's first data embassy in Luxembourg." *e-Estonia Briefing Centre.* 14 Jun. https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/.

Egan, Brian J. 2017. "International Law and Stability in Cyberspace." *35 Berkeley Journal of International Law* 169-180. https://scholarship.law.berkeley.edu/bjil/vol35/iss1/5/.

Gellman, Barton, and Greg Miller. 2013. "'Black budget' summary details U.S. spy network's successes, failures and objectives." *The Washington Post.* 29 Aug. https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.

Kaljulaid, Kersti. 2019. "President of the Republic at the opening of CyCon 2019." *President of Estiona.* 29 May. https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/.

Koh, Harold Hongju. 2012. "International Law in Cyberspace." *USCYBERCOM Inter-Agency Legal Conference.* Faculty Scholarship Series, 18 Sep. https://digitalcommons.law.yale.edu/fss_papers/4854.

Kundra, Vivek. 2010. “25 Point Implementation Plan to Reform Federal Information Technology Management.” *U.S. Department of Homeland Security.* 09 Dec. https://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf.

Ministère des Armées. 2019. “Droit internatinoal appliqué aux opérations dans le cyberspace.” *Ministère des Armées, Répulique française.* 2 Sep. https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf.

O'Sullivan, Dan. 2019. “Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online.” *UpGuard.* 16 Aug. https://www.upguard.com/breaches/cloud-leak-inscom.

—. 2019. “Dark Cloud: Inside The Pentagon's Leaked Internet Surveillance Archive.” *UpGuard.* 23 Aug. https://www.upguard.com/breaches/cloud-leak-centcom.

—. 2019. “Insecure: How A Private Military Contractor's Hiring Files Leaked.” *UpGuard.* 27 Sep. https://www.upguard.com/breaches/cloud-leak-tigerswan.

Schmitt, Michael, and Liis Vihul. 2017. *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge Univeristy Press.

Shared Services Canada. 2019. *Cloud services.* 13 Aug. https://www.canada.ca/en/shared-services/corporate/cloud-services.html.

—. 2019. *Twitter.* 9 Aug. https://twitter.com/SSC_CA/status/1159869302507540480.

Solis, Gary. 2016. *The Law of Armed Conflict: International Humanitarian Law in War.* 2nd. Cambridge: Cambridge University Press.

Thuppal, Raj, and Dinesh Mohan. 2017. “Memorandum to the Chief Operating Officer: Storing Government of Canada Data Outside of Canada.” *Document Cloud.* May. http://s3.documentcloud.org/documents/3988530/Cloud.pdf.

Treasury Board of Canada Secretariat. 2019. “2019-20 Estimates: The Government Expenditure Plan and Main Estimates.” *Government of Canada.* 29 Mar. https://www.canada.ca/content/dam/tbs-sct/documents/planned-government-spending/main-estimates/2019-20/me-bpd-eng.pdf.

—. 2019. “Digital Operations Strategic Plan: 2018-2022.” *Government of Canada.* 29 Mar. https://www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html.

—. 2017. “Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021.” *Government of Canada.* 28 Nov. https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/strategic-plan-2017-2021.html.

—. 2019. “Government of Canada White Paper: Data Sovereignty and Public Cloud.” *Government of Canada.* 17 Jun. https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html.

U.S. Department of Justice. 2019. “U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online.” *U.S. Department of Justice.* 3 Oct. https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

U.S. Government Accountability Office. 2014. “Cloud Computing: Additional Opportunities and Savings Need to Be Pursued.” 24 Sep. www.gao.gov/assets/670/666133.pdf.

United States of America v. Microsoft Corporation. 2018. 17-2 (Supreme Court of the United States, 17 Apr).

United States of America, petitioner v. Microsoft Corporation, Petition for a writ of certiorari. 2017. 17-2 (Supreme Court of the United States, 29 Sep).

Wright, Jeremy. 2018. “Cyber and International Law in the 21st Century.” *Chatham House Royal Institute for International affairs.* U.K. Attorney General's Office, 23 May. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

