WFH, not WTH? The security challenges of working-from-home

Neal Kushwaha[1], Piret Pernik[2] and Bruce W. Watson[3]
[1]IMPENDO Inc., Ottawa, Canada
[2]Strategy Branch, NATO CCDCOE, Tallinn, Estonia
[3]IP Blox and IMPENDO Inc., Eindhoven Netherlands and Ottawa, Canada
neal@impendo.com
piret.pernik@ccdcoe.org
bruce@ip-blox.com and bruce@impendo.com

Abstract: Under the coronavirus pandemic, governments and corporations around the world have adopted a work-from-home (WFH) mode of operations to continue governing and operating. Over a two year into the COVID-19 pandemic, many of us continue to work from home and a large majority have few plans to return to the office. Early on, governments and companies scrambled to increase Virtual Private Network (VPN) licenses and bandwidth capacities to take on the additional user load at a technical level. This allowed a near seamless continua of communications for common government unclassified information and corporate sensitive information of non-national interest using commercial software encryption. But what about information of national interest? A smaller number of individuals in key government departments, sometimes under staff rotations, continued to work in the office to serve these needs. Within weeks, government departments began deploying assets to access classified Secret systems from home. This paper discusses the WFH use of classified (e.g., Secret) IT systems while considering multiple security areas (physical, operational, personnel, IT, communication, and electromagnetic and radio-frequency emission) with focus on insider threats and foreign state actors, to describe the impact to the WFH public servant, the citizens, and the government. It describes the severe security challenges and risks governments have accepted under the pandemic, raising the question "*what the heck* were governments thinking?"

Keywords: work from home, government, insider threats, foreign state actors, national interest

1. Introduction

The COVID-19s pandemic has reshaped the way businesses and governments operate. Even with the ability to do it remotely, many companies have been permanently shut. The *work from home* (WFH) method of conducting business operations *wherever possible* has become the new way of working for many, including governments. Never has there been an event to drive a global WFH during the information age. While some research has been performed under the notion of working from home (Giri 2022) (Carvin 2021) (Vériter, et al. 2021), the research into the negative impact to national interests due to classified WFH has not been described.

Each government designs, manages and implements policies to categorise information. These categories closely align to their foreign counterparts, but still remain different. In Canada, it is categorised as follows (Treasury Board of Canada Secretariat 2019a):

1. Unclassified: normally information that has been declassified, is of low value, and has negligible-to-low impact if released; the information may already be publicly available; in some states, the term also means the information referenced is "not yet classified" while in others, it includes the information classified for internal use.
2. Non-national interest: in various states, this information is still considered unclassified but includes other designations to represent its sensitivity; across various States, the designation is represented by terms such as RESTRICTED (e.g. USA), PROTECTED (e.g. Canada), OFFICIAL, INTERNE, SBU (*sensitive but unclassified*), and others; non-national interest information is of low impact to the state but can be of varying degrees of impact to an individual including physical injury, kidnapping, and loss of life.
3. National interest: this category is commonly subcategorised into three in Canada (Treasury Board of Canada Secretariat 2019a) or four sub-containers at NATO and other states (Estonian National Security Authority n.d.); while each sub-container's classification label is not strictly agreed upon by all governments, for purpose of this paper, the level of general understanding described below is adequate.
   - RESTRICTED;
   - CONFIDENTIAL: release of information is likely to cause injury to the national interest;
   - SECRET: release of information is likely to cause grave injury to the national interest; and
   - TOP SECRET: release of information is likely to cause exceptionally grave injury to the national interest.

Government civil servants compose and share various documents that are restricted on access by legislation even while in draft. Governments maintain procedures, regulation, and laws within which national interest information is created, transmitted, stored, and destroyed at a common standard across all its branches. Other sub-controls exist to further limit the exposure of the information impacting national interest, for example dissemination controls (e.g., TOP SECRET//CANADIAN EYES ONLY, or TS//CEO in short form).

Under Canadian legislation, lead security agencies (Treasury Board of Canada Secretariat 2019b) of the federal government provide guidance that national interest information should not reside or be transmitted in *plain text* (or *in the clear*) on publicly accessible networks and that each of the systems that carry national interest information must adhere to increasingly strict security controls as the injury to the national interest increases (Canadian Centre for Cyber Security 2018).

The content creator is commonly responsible to classify the information and that is one of the many reasons why information is incorrectly classified. While domestic laws exist to manage the release of national interest information, in some states including Canada, governments must prove intent in order to convict. Since classified information is only available in *plain text* on government physically isolated systems,[1] the greatest threat to the confidentiality, integrity, and access remains with the users, who are considered insider threats. Insider threats can release information (1) without intent, (2) intentionally without malice, and (3) with malicious intent.

Security professionals with traditional experience come together with technological experienced security professionals to help mitigate and safeguard the threat and risks that states face. To facilitate reading the remainder of the paper, we define these security domains[2] as follows.

1. Non-technological security domains:
    - Physical security (PhySec): the practise of securing people and assets from unauthorised access and natural threats that result in a breach of confidentiality, damage, or loss.
    - Operational security (OPSEC): the assessment and protection of publicly available information and observable behaviours, that when collectively analysed by an adversary, disclose compromising information or information that was intended to remain undisclosed.
    - Personnel security (PERSEC): the evaluation of an individual's reliability, loyalty, and trustworthiness; it also discloses how the individual can be compromised, discredited, and even eliminated.
2. Technological security domains:
    - IT security (ITSEC): a discipline concerned with protection of information technology using tools, policies, procedures and more from unauthorised access.
    - Communications security (COMSEC): a discipline that ensures secure electronic transmittal of information, while preventing unauthorised access using cryptography.
    - Emission security (EMSEC): the practise to identify and reduce the interception of signal emissions from technological equipment.

In WFH conditions, the challenges in each of these categories are as follows:

1. PhySec: Physical security policies (how to define security zones and controls at home).
2. OPSEC: Operational security policies (difficult for the security office to oversee users working from home).
3. PERSEC: Personnel security challenges (new people at home potentially having access or awareness of information and possibly how to access the information).
4. ITSEC: IT security considerations (exponential growth in sources of entry, and thus attack surface).
5. COMSEC: Communication security doctrine (complications in granting access to COMSEC equipment from home).
6. EMSEC: Electromagnetic and radio-frequency emission security concerns (greater threat from uncontrolled homes versus well-spaced and protected government campuses).
7. Insider threats: Users can likely bring other devices into the frame such as cameras to capture screens and share information through other means that are out of the control of the government.

[1] Isolated and private networks can still be globally accessible.

[2] These security domains are very intermingled, e.g., communications security professionals consider threats and risks related to physical security, operations security, personnel security, and emission security.

8. Foreign state actors: With many foreign state actors unable to travel to countries and within countries, how might they use other means to exploit individuals (sabotage) and exfiltrate information (espionage) and continue with their mission?

Under the pandemic, the norms of safeguarding restricted information have been relaxed, increasing the threat of domestic and foreign espionage and sabotage. Phone calls that were *never* made on open public telecom infrastructures are now being held on public mobile phones in order to continue governing, for example under the US NETCOM, the US Army will deploy access to SIPRNet (classified SECRET) for over 2000 users (Eversden 2020). In some cases, tactical conversations with minimal cover-time may be justified due to low risk, however, strategic ones with greater cover-time and greater risk remain much more difficult to justify. The same issues apply to documents of national interest over public transports (e.g., Internet).

Our paper describes the various risks that are being accepted by governments, as they authorise national interest information to be created, shared, stored, and destroyed outside of their common controls at home.

The following sections will outline these non-technological and technological risks by illustrating them with commonly used WFH scenarios.

2. Non-technological security

When we think of government facilities, swipe cards, security guards, bollards, cameras, and more come to mind. Government offices come in a varying degree of styles and locations. Regardless of where the building is situated, it is an obvious source of Physical Security (PhySec), Operations Security (OPSEC), and Personnel Security (PERSEC) information for observers to ascertain.

Simple matters can be understood by simply watching the resources entering and exiting the campus or building(s). Their mode of transportation to and from may include for example, public transit or vehicle make and model, which can help ascertain one's income and if followed home, can help identify where they live, the type of home in which they live, their dependents, and other habits they may have.

Facility data that can be gathered from simply watching the resources enter a campus or building(s) include working hours of the resource, general working hours of the facility, ingress and egress points of the facility, and specific entry points for office workers, maintenance resources, and even deliveries. Based on the type of site or department hosted in the facility, the facility clearance level may also be ascertained and thereby the likely level of clearance granted to those who enter and exit the facility on a regular basis. Resources entering the campus or facility often must present a badge and most resources do not pocket or hide their badges while off campus. Some badges indicate clearance levels or status of the resource (through colour coding or possibly simply letters), thereby offering further data to the adversary watching from a far.

Resources arriving in seemingly professional, or business attire may indicate a more senior level resource, regular casually dressed resources may indicate a general civil servant, whereas a resource in uniform may indicate defence related or possibly facilities management resources.

Once an adversary identifies a resource as a valuable asset, they can gather much more specific data through targeting tradecraft.

In the few bullets above, the surveillance at the external PhySec layer of the facility ties closely to OPSEC and PERSEC. Open and unoccupied land surrounding a building help the departmental security team by offering time to intercept a perpetrator that may be approaching, trespassing, or climbing over a distant perimeter fence, while layers of fencing can slow the perpetrator. The private roads on the campus help control access and allow for the security team to evict unauthorised or suspicious vehicles, and potential observers (in vehicles or as pedestrians).

Considering only the three security principles above, if a civil servant with security clearance (granted to access and compose classified materials) were to *work from home* under the pandemic after only having worked at the office for years, they would likely not have access to equipment or methods to connect to their government departmental services to work on national interest matters from home. The civil servant may not have a portable

device of any kind to work from home because their normal workplace has always been in a secure government facility authorised for such classified workloads.

2.1 Scenario 1: WFH with authorised government equipment

Under normal working circumstances, in order to consume and/or create classified materials, the civil servant would need to travel to work to use classified compute devices. In this scenario, under the pandemic restrictions, the civil servant would need to (1) travel to the office to pickup authorised telework devices (or classified WFH kit) to be used from their residence, or (2) have authorised personnel from the office travel to the civil servant's residence to deliver and/or install telework devices (or classified WFH kit). In the latter two cases, the government department must already have the technological capability in place to offer the civil servant access to the national interest collaboration environment through secure telework communication capacities.

In any case, if the civil servant was already a target by a domestically located foreign threat actor, their behaviour at home is likely already known and if they are not already a target, working from home during the pandemic might not be a grave physical security risk. Or is it?

If the civil servant has been granted equipment to securely and remotely access and collaborate on matters of national interest (e.g., equivalent to classified SECRET such as the US and their WFH deployed access to SIPRNet), many questions arise.

A skilled PhySec resource should be consulted to ascertain the risks associated with the residence. The type of residence, e.g., an apartment building, a semi-detached, or single home, introduces different types of considerations and concerns. Each will most likely require further investigation into the neighboring residents and their affiliations, but more so for the apartment buildings and semi-detached buildings.

The PhySec resource would also assess the physical construction of the residence and measure them to a government facility standard required to host classified assets. For example: wall and floor construction using reinforced concrete versus wood and/or poly structure, steel doors and steel door frames attached to steel studded walls, and window frames along with windows lined with film to limit and deter break entries.

Government facilities are constantly monitored by an authorised group of individuals skilled at handling incidents and intercepting individuals who may be lurking or attempting to breach the perimeter, long before they reach the facility. The PhySec resource assessing the residence would likely assess the security controls surrounding the home, such as sensors and their coverage of all access points, wired or wireless sensors and battery maintenance, and intrusion alarm systems. They would additionally assess whether such systems are normally armed even when the residence is occupied, who has access to enable or disable the alarm system, the presence of camera systems and where they are pointed, as well as who has access to recordings and how is the recorded information accessed, etc. While it is nice to have these controls in a residence, they often do not meet the standard of a government facility set of controls. Challenges such as response time, continuous monitoring by a government resource (as opposed to a private sector company), and where the data is stored (e.g., public cloud repositories for security and camera feeds, or closed circuit) are just a few of the concerns.

Once the perimeter and overall home construction is reviewed, the precise location of the classified asset(s) must be identified so that further assessment can be made by the PhySec resource. In some cases, this may require allocating a room within the residence that has no windows and preferably not attached to the exterior walls of the residence. The room may require further construction to secure the door, door frame, internal walls, WiFi signals, listening devices or digital assistants (e.g., Amazon Alexa, Apple Siri, or Google Assistant), and more. In some cases, these types of rooms may not exist in a residence. In many cases, the use of a security container may be required to store the classified asset(s) and safeguard the injury level of the data-at-rest or access to the data, and such a security container may require a near permanent attachment to a concrete surface.

Even after noting these deficiencies, the government may not have the ability to fund the construction or procure the assets required in civil servant's residence, as there are further concerns for liability as well as differences between ownership and rental of the residence, along with the optics of spending of taxpayer monies to fund the construction in a civil servant's residence, to name just a few.

The PhySec resource will likely work closely with a government authorised PERSEC resource to ensure that all residents of the home (over a certain age) who may have access to the classified assets be cleared and granted the appropriate level of personnel clearance required (e.g., SECRET clearance). Such requirement would most likely also apply to anyone who may have access to the residence, e.g., friend, family member, maintenance company, or landlord who maintains a key and/or security alarm code to the residence.

To clear all these resources to the appropriate level required (as they may have access to the residence and therefore extended amount of time to gain access to the classified assets without being noticed) would be a difficult task under normal circumstances and take even longer during a pandemic.

Finally, the civil servant will most likely require OPSEC training to ensure they perform specific actions before use, after use, and while away from the residence hosting the classified assets. This can include where to use the assets, when to use the assets, not using them near any wireless access points, windows, into cameras, around others, disconnect other electronic equipment in the residence, and more.

Resources skilled in securing government facilities will most likely mark any residence and their occupants as an elevated risk and not recommend the location for consumption or creation of classified information, or storage of assets that may access classified resources.

As can be ascertained from the content above, PhySec, OPSEC, and PERSEC evaluations should be performed by trained and skilled individuals to measure the likelihood and thereby risk of a variety of matters including (1) the theft of the access and assets to (2) coercion by another party to the sale of access (or the assets) by the civil servant to another party.

For a government department to measure these risks, they would likely need a large team to visit the residences, interview the civil servant, and ensure mitigations are in place prior to granting secure remote access, raising the follow-up question: who is responsible to fund the travel and these mitigations? All the while the government is likely strongly advocating physical distancing policies and enforcing inter- and intra-city travel restrictions.

Under these travel restrictions, it would be challenging for an adversary to physically target the civil servant at their home (e.g. parabolic dish with microphones from inside nearby vehicles, low-powered voice and/or video capture and transmitting devices located in on windows, or walking up to the property and residence), however, if for example the civil servant was considered a high value target prior to the pandemic and resides in a high-rise or other shared complex, the neighbouring apartment may already be occupied by a well-funded adversary.

The non-technical security threats and risks that government facilities face are well understood and managed by the traditional security community. Safeguards that can be easily employed at an office are very challenging to construct and impose in a home, and in may even be restricted by state laws.

3. Technological security

Today's homes are filled with technological capabilities that would never be present in a government facility where matters of national interest are discussed and shared. Voice controlled home automation (e.g., Amazon Alexa, Apple Siri, or Google Assistant), personal security and alarm systems, poorly- or un-maintained residential hardware and software products, in-home and neighbouring Wi-Fi access points, electromagnetic interference, poor password controls and more plague the residence and consumer market.

At a high level, a possible communication path from the residence to the office could be (1) a State controlled and authorised national interest information compute device (e.g. terminal, phone, computer) communicating via (2) a state controlled and authorised cryptographic assets (algorithm, keys, and hardware) protected by (3) a state controlled and authorised firewall to (4) a government compute facility that mirrors the layers of the Communications Security (COMSEC) and IT Security (ITSEC) described.

The Figure 1 below depicts a high-level example of a classified WFH kit (e.g., SECRET) supporting information communications in red and state encrypted and safeguarded communications (via algorithms, keys, and hardware) over public networks in black communicating to-and-from the office.

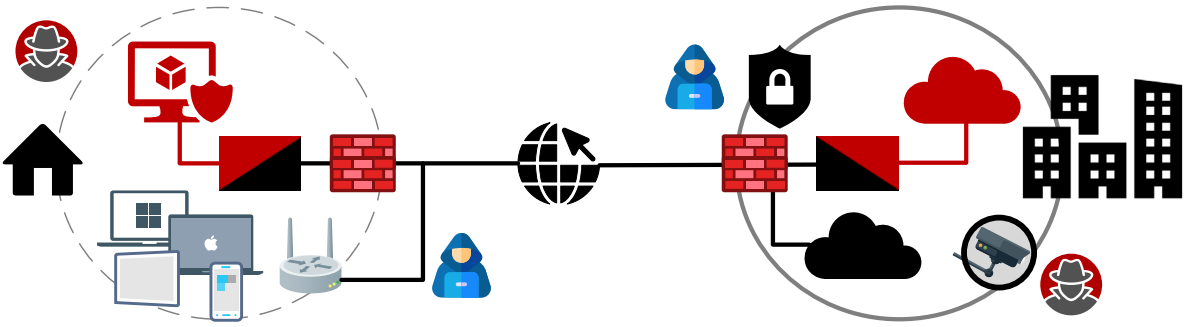

Figure 1: High level example of a secure communication path from the home to a government office

In such a case, home users would be granted access to classified networks (e.g., SECRET) using a classified WFH kit via a user account with defined security controls to and through the respective authorised classified device located in their residence. Governments may decide to grant new remote-access-only accounts created specifically with very limited access to national interest information systems and very limited functionality (e.g., no printing, no injection or extraction of data, mandatory card-and-PIN access) to minimise the possible exposure of confidentiality and adverse impact to data integrity. Governments may also impose additional ITSEC policies and safeguards using mature security logging, monitoring, analytics, alerting, active defence, multifactor authentication, zero-trust capabilities, and other technologically supported capabilities.

No matter what technological oversight (security monitoring) or controls used, certain mitigations from the home will simply not be possible without correlation of information from PhySec, and even then, the risk of information exposure could remain high. For example, it would be impossible to know if the resource *actually used* their credentials to access the system or if another person is using it on their behalf (insider threat).

3.1 Scenario 2: Insider threat

A common cybersecurity risk to any organisation is insider threat. As per recent research, almost 30% of cyber attacks are estimated to be conducted by an insider, but insider threats need not be cyber-based (see https://resources.sei.cmu.edu/asset_files/SpecialReport/2005_003_001_51946.pdf).

A civil servant using a classified WFH kit could choose to turn against their state by:

1. capturing photographs or video camera footage of the on-screen classified information, and/or
2. inviting foreign state adversaries into the residence to use the device and access and possibly even alter national interest information through the civil servant's credentials.

In either of these cases, there is little the government can do to notice this behaviour through IT security monitoring of the access by the civil servant from their residence.[3] Even when using very mature methods of IT security monitoring, correlation, analytics, and forensic analysis, these two behaviours mentioned above would not be detected as they exhibit expected and normal use of a common user's access. Furthermore, regular use of search tools by the user and opening random documents becomes the baseline for this user, then behaviour analytics tools may overlook this user's behaviour. If the user is called in an interview to validate their actions, they could cover it by stating the available information management search tools are terrible and force the user to open and read too many documents to find the required information. While limits and access controls applied to user accounts may be considered good practise, it is not necessarily common practise.

3.2 Scenario 3: RF and EM interference

At a radio frequency and electromagnetic level, when commercial off the shelf (COTS) equipment is used for the end-user compute device in the residence, the electromagnetic signals emitting from the device's display (Kuhn 2005) and each keystroke (Vuagnoux and Pasini 2009) can be captured and easily deciphered by a technically inclined high-school or college student using equipment readily available from common Internet sources mixed with some home-made antennas. Depending on the type of residence, some EMSEC exploits (spatially and conducted emanations) can be particularly obvious to spot.

[3] Breach of confidentiality could be to a foreign state, multi-national or domestic corporation for corporate advantage, or even anonymously to the public. The breach of confidentiality need not be for financial gain.

If TEMPEST (National Institute of Standards and Technology (NIST): Computer Security Resource Center (CSRC) n.d.) end user equipment is being considered to mitigate EMSEC attacks at the residence, the physical security of the TEMPSET tested and certified equipment becomes very important. The user of the equipment will need to remain aware of any tamper to the equipment and be vigilant in carrying out all PhySec policies and procedures along with possibly state COMSEC doctrine. If the state is unable to adequately control the physical space where the TEMPEST equipment is located and used, then the use of TEMPEST is of little use. Adversaries with close access to the TEMPEST equipment need not use EMSEC methods to gain access to the national interest information. Various low-cost screen capture and keyboard capture/injection devices can be purchased online that are easily connected inline with display and keyboard cables. These capture and injection devices can allow an adversary to record any activities, be notified when end user activity is detected, and watch live or review all the recorded activity from a repository in the cloud using commercially available tools such as "Screen Crab" and "Key Croc" (Hak5 n.d.).

3.3 Scenario 4: Use of COTS

Governments may believe COTS equipment, COTS cryptographic algorithms, and certificates are adequate for safeguarding their national interest information under the WFH policy, possibly with other safeguards and limited access. In such cases, the use of side channel attacks and fault injection attacks offer a remote method to capture cipher keys (secret keys) from compute devices when they are normally used by the residential user using commercially available tools such as the Rambus DPA and SPA workstation side channel attack platform (Rambus Inc. n.d.).

These side channel attacks use differential power analysis of a cryptographic device. As an example, devices need to be powered on, can be in "airplane mode," and accessing their secret key. With enough data, today's compute capacities can detect very small similarities and extract AES, RSA, DES, and other ciphers on various devices including FIPS 140-2 and 140-3 certified units. With a cipher key in hand, the adversary opens the door to other options for espionage and sabotage. Side channel attacks can be effective with various compute devices (e.g., mobile devices, dedicated cryptographic devices, computers, Internet of things, terminals).

For example, if states only consider some of the security domains (e.g., COMSEC and ITSEC) and focus on adversaries breaching their systems primarily through mathematical means, they will likely miss out on safeguarding the national interest information. When one considers the types of adversaries trying to acquire national interest information, ignoring these risks can prove to be very dangerous.

4. Discussion

During the questions and answers after his speech on August 8, 2017, at the annual *Space and Missile Defense Symposium* in Huntsville, Alabama, General John Hyten, now Vice Chairman of the Joint Chiefs of Staff and in 2017 commander of US Strategic Command (USSTRATCOM), stated (U.S. Strategic Command 2017):

> *"There's no such thing as a war in cyberspace. There's just war. We have to figure out how to defeat our adversaries, not to defeat the domains that they operate in. So we need capabilities and we need technologies to stay ahead of our adversaries in each one of those elements."*

His quote was in response to a question on the USSTRATCOM's priorities. When applied to securing government information during WFH, defending one security domain at a time (PhySec, OPSEC, PERSEC, ITSEC, COMSEC, or EMSEC) is not a good defence. Adversaries will attempt to breach all domains at the same time.

Combining the non-technological and technological domains, adversaries can not only gain access to more information (deeper into the organisation or individual), but also use these capabilities to gain access to their target's trusted parties (wider scope). A good example of this is the recent supply chain integrity vulnerability that we all experienced via the SolarWinds cyber attack, impacting nearly 18,000 of their customers (Porter 2021). In this case, the adversary's target was not just SolarWinds (Tidy 2020). It was most likely many of the suppliers of government services, e.g., FireEye (FireEye Inc. 2020) and Microsoft (MSRC Team 2020), to allow for multiple points of entry into 250 branches of governments and suppliers (Porter 2021).

Under the political challenges of the coronavirus pandemic, governments around the globe have made concessions so that their governments may continue to govern, as the US Army did when they deployed access to SIPRNet for over 2000 users (Eversden 2020). The priority to (1) maintain public health and the ability to

earn/spend, (2) uphold international agreements, and (3) maintain a reliable economy with a stable state currency is critical. Losing any one of those three will crumble the remaining two.

At the February 17, 2021, UN Security Council open meeting on *Ensuring Equitable Access to COVID-19 Vaccines in Contexts Affected by Conflict and Insecurity*, UN Secretary-General António Guterres stated (Guterres 2021):

> *"Yet progress on vaccinations has been wildly uneven and unfair. Just 10 countries have administered 75 per cent of all COVID-19 vaccines. Meanwhile, more than 130 countries have not received a single dose."*

Secretary-Generals Guterres' remarks are a reminder that if states do not work together to manage the coronavirus pandemic, only a small number of states will have administered the COVID-19 vaccine broadly (10 countries). That means, many states will not be positioned to retract their "national interest WFH" decisions for a long time.

For example, the costs to retrofit a government building to mitigate risks of all security domains is very high, and the timeline to achieve these safeguards is significantly longer than deploying a classified WFH kit to under 100 WFH civil servants. Indeed, they are not the same, but in the latter case, government operations can immediately deliver value to its citizens, whereas in the other, it could take years to begin. As states release a classified WFH capability, much like the US Government has done with SIPRNet, they may wish they never opened Pandora's box.

In October 2019, the Global Health Security Index report (Global Health Security Index 2019) measured 195 countries for their ability to survive a global epidemic or pandemic – based on their preparedness and playbooks. The actual results thus far during the coronavirus pandemic differs greatly from that report's projections. Have such preparations and playbooks provided false guidance to governments? We can only hope the pandemic serves as a learning opportunity for governments to review federal disaster plans, test their capabilities, and spend the time to pre-think for the future.

5. Conclusion

We live in a world where certain governments have accepted the high risks to a variety of threats with their WFH policies. If a foreign state sponsored adversary makes their way in, who knows how long they will be able to linger and how deep and wide their impact will be. Maybe, by the time any breach surfaces, democratic governments will have changed hands. Regardless of how the governments react and respond after the breach, the impact to confidentiality, integrity, and access may have already been realised.

The global coronavirus pandemic has mostly resulted in a chaotic response from governments and corporations with their respective WFH policies. These WFH methods may seem adequate for matters of non-national interest, however, even with encryption safeguards, national interest WFH has led us to wonder "what the heck" have we done.

States whose citizens are near fully vaccinated can return to processing matters of national interest in the safety and safeguards offered by their government facilities, hopefully terminating any classified WFH capabilities that may have been adopted. The longer it takes for states to vaccinate their citizens, the longer the government national interest WFH policies will remain in effect, leaving (1) governments as an even bigger target for domestic and foreign espionage and sabotage, and (2) the civil servants with classified WFH access an obvious and arguably easier target. Although not discussed in this paper, similar challenges can be extended to critical national infrastructure and industries.

References

Canadian Centre for Cyber Security. 2018. *IT Security Risk Management: A Lifecycle Approach (ITSG-33).* 05 November. Accessed December 12, 2021. https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33.

Carvin, Stephanie. 2021. "Canadian National Security Operations during COVID-19." Chap. 6 in *Stress Tested: The COVID-19 Pandemic and Canadian National Security*, 107-126. Calgary: University of Calgary Press. Accessed December 12, 2021. https://prism.ucalgary.ca/bitstream/handle/1880/114134/9781773852447_OA.pdf?sequence=1#page=117.

Estonian National Security Authority. n.d. *Comparative Tables.* Accessed December 12, 2021. https://www.valisluureamet.ee/nsa/tables.html.

Eversden, Andrew. 2020. “The Army will soon allow users to access classified info from home.” *C4ISRNet.* 22 June. Accessed December 12, 2021. https://www.c4isrnet.com/2020/06/22/the-army-will-soon-allow-users-to-access-classified-info-from-home/.

FireEye Inc. 2020. “Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.” *Mandiant Inc.* 13 December. Accessed December 12, 2021. https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

Giri, Susma. 2022. “The Impact of Covid-19 on National Security of Nepal.” *Unity Journal* 2: 236-264. Accessed December 12, 2021. doi:https://doi.org/10.3126/unityj.v2i0.38852.

Global Health Security Index. 2019. “2019 Global Health Security Index.” 20-29. Accessed December 12, 2021. https://www.ghsindex.org/wp-content/uploads/2020/04/2019-Global-Health-Security-Index.pdf.

Guterres, António. 2021. “Secretary-General's remarks to the Security Council Open Meeting on Ensuring Equitable Access to COVID-19 Vaccines in Contexts Affected by Conflict and Insecurity [as delivered].” *United Nations.* 17 February. Accessed December 12, 2021. https://www.un.org/sg/en/content/sg/statement/2021-02-17/secretary-generals-remarks-the-security-council-open-meeting-ensuring-equitable-access-covid-19-vaccines-contexts-affected-conflict-and-insecurity-delivered.

Hak5. n.d. *Hak5 Official Site.* Accessed December 12, 2021. https://shop.hak5.org/.

Kuhn, Markus G. 2005. “Electromagnetic Eavesdropping Risks of Flat-Panel Displays.” In *Privacy Enhancing Technologies: 4th International Workshop, PET 2004, Toronto, Canada, May 26-28, 2004. Revised Selected Papers*, 88-107. Berlin: Springer. Accessed December 12, 2021. doi:https://doi.org/10.1007/11423409_7.

MSRC Team. 2020. “Microsoft Internal Solorigate Investigation Update.” *Microsoft Security Response Center (MSRC).* 31 December. Accessed December 12, 2021. https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/.

National Institute of Standards and Technology (NIST): Computer Security Resource Center (CSRC). n.d. *Gloassary: TEMPEST.* Accessed December 12, 2021. https://csrc.nist.gov/glossary/term/TEMPEST.

Porter, John. 2021. “White House now says 100 companies hit by SolarWinds hack, but more may be impacted.” *The Verge.* 18 February. Accessed December 12, 2021. https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies.

Rambus Inc. n.d. *DPA Workstation Analysis Platform.* Accessed December 12, 2021. https://www.rambus.com/security/dpa-countermeasures/dpa-workstation-platform/.

Tidy, Joe. 2020. “SolarWinds Orion: More US government agencies hacked.” *BBC News.* 15 December. Accessed December 12, 2021. https://www.bbc.com/news/technology-55318815.

Treasury Board of Canada Secretariat. 2019a. *Directive on Security Management - Appendix J: Standard on Security Categorization.* 01 July. Accessed December 12, 2021. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32614.

—. 2019b. *Policy on Government Security, Chapter 5.* 01 July. Accessed December 12, 2021. https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578#cha5.

U.S. Strategic Command. 2017. *General John E. Hyten Speech, Space and Missile Defense Symposium.* 08 August. Accessed December 12, 2021. https://www.stratcom.mil/Media/Speeches/Article/1274339/spaceand-missile-defense-symposium/.

Vériter, Sophie L., Monica Kaminska, Dennis Broeders, and Koops Koops, . 2021. *Responding to the COVID-19 ‘infodemic’: National countermeasures to information influence in Europe.* The Hague: The Hague Program for Cyber Norms. Accessed December 12, 2021. https://www.thehaguecybernorms.nl/news-and-events-posts/responding-to-the-covid-19-infodemic-national-countermeasures-against-information-influence-in-europe.

Vuagnoux, Martin, and Sylvain Pasini. 2009. “Compromising electromagnetic emanations of wired and wireless keyboards.” *18th USENIX Security Symposium.* 1-16. Accessed December 12, 2021. https://www.usenix.org/legacy/events/sec09/tech/full_papers/vuagnoux.pdf.