HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on National Defence

NDDN • NUMBER 065 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, October 25, 2017

Chair

Mr. Stephen Fuhr

Standing Committee on National Defence

Wednesday, October 25, 2017

● (1530)

[*English*]

The Chair (Mr. Stephen Fuhr (Kelowna—Lake Country, Lib.)): I'd like to welcome the committee to our final hearing on the crisis in Ukraine and to welcome our three panellists to round out today's discussion on this issue: Alan Bell, president of Globe Risk International; Stuart Wright, chief information security officer, Aegis Technologies, appearing as an individual; and we're still waiting on Viktor Siromakha. We'll put him last on the speakers list so that we can get started.

Thank you, everybody. I understand you've been briefed on the 10-minute limit. I would very much appreciate it if you try to stick to that as closely as possible so that I can give the members the opportunity to ask questions.

Mr. Wright, you have the floor.

Mr. Stuart Wright (Chief Information Security Officer, Aegis Technologies, As an Individual): First, I want to thank the panel for requesting my presence here in Ottawa to brief these distinguished parliamentary members.

My name is Stuart Wright. I'm attending today as an individual.

I have worked in regulation; energy including oil and gas transmission, distribution, and generation; and audit and information systems in different leadership capacities for many years. I have a degree of expertise and a unique perspective on cybersecurity here in North America.

I'm here today to provide a layman's briefing on the events in the Ukraine and eastern Europe as they relate to cybersecurity. My hope is that this will inform the panel as they assess the appropriate measures and next steps to support our NATO allies and enhance Canada's military capability to respond to a new type of warfare.

This week's cyber-attacks using malware called Bad Rabbit hit Russia and other nations on Tuesday, affecting the Interfax news agency and causing flight delays at Ukraine's Odessa airport. The Bad Rabbit ransomware is a type of virus that locks up infected computers and asks victims to pay a ransom to restore access. While no major outages were reported, several governments have issued warnings on the attack, which followed campaigns in May and June that used similar malware and resulted in what some economists have estimated are billions of dollars in losses. These new rounds of attacks are disturbing because attackers quickly infected critical infrastructure, including transportation operators, indicating it was a well-coordinated attack.

Some cybersecurity firms have indicated that Bad Rabbit appeared to spread through a mechanism similar to June's disruptive NotPetya virus, which took down many Ukrainian government agencies and businesses. It then spread across corporate networks of multi-nationals with operations or suppliers in eastern Europe. According to early reports on Bad Rabbit, more than half the victims were in Russia, followed by Ukraine, Bulgaria, Turkey, and Japan.

I'd now like to speak to the Ukraine cyber-attack of 2015, as you requested. On December 23, 2015, unknown cyber-forces disrupted energy grid operations for first time, causing large blackouts over 225,000 customers in Ukraine. It affected several regions in the country, which went without power for several hours. This was facilitated by malware called BlackEnergy.

In December 2016, almost exactly one year later, there was another blackout, smaller in scale and lasting only one hour. It hit only one region but was conducted with a more advanced malware, Industroyer, which is suspected to be the cause in this case.

These cyber-incidents impacted operators in the electricity sector, but the tactics used in these attacks could have easily played out against any operators in any sector and in any jurisdiction in any country. The bottom line here is that cyber-threats are no longer the concern of IT network administrators and engineers but must be a central concern in running a safe, efficient, and resilient critical-infrastructure operation.

I'd now like to talk about the global landscape. Global cyber-attacks are now concerted. They're orchestrated efforts to exploit vulnerabilities in people, systems, and processes. They're impactful, long-lasting, and often professional efforts to use an organization's network infrastructure against it in a highly targeted way.

In the traditional understanding of war, critical infrastructure was a sound target of opportunity: hamper the ability of the opponent to utilize it, thus rendering it useless. Public Safety Canada defines critical infrastructure as “processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.” The disruption of any critical-infrastructure provider could potentially result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. In other words, critical infrastructure is an ideal and easy target.

Historically, critical infrastructure was easy to defend, as it was available via air-, land-, or sea-based assets of an opponent. The deployment of such capabilities can result in the potential transmitting of movement, and even if the exact target is unknown, can be limited by conventional defensive capabilities. This was particularly relevant in the era of state-versus-state war such as the bombing campaigns we witnessed during the Second World War and the later political-military conflicts of the latter 20th century.

In the modern geopolitical era, however, there is another dimension of assets now operating within the cyber-realm with near global reach and little to no movement of efforts. Effectively, the nature of war and conflict has evolved. These cyber-assets are now deployable quickly and are never physically exposed to the opponent. They are able to target critical infrastructure from within the borders of their state or through third-party proxies, utilizing techniques, tactics, and procedures, TTPs, to carry out effective assaults on their targets.

The Department of National Defence, its partners in NATO, and strategic allies in Europe, Asia, and south of the border need to revisit the military doctrines required to effectively guide cyberwarfare strategies. These include our capabilities and core elements of training, intelligence, and support to ensure security and stability of our allies and regional partners.

● (1535)

The same TTPs separate the average cybercriminal from more sophisticated threat actors, and these advanced persistent threats, APTs, are effectively a set of stealthy and continuously computing hacking processes orchestrated by a person or persons targeting a specific entity.

An APT usually targets either private organizations, states, or both. The targeting of critical infrastructure or state-based assets by APTs may include financial institutions; energy systems; transport automation; water and waste-water management; as we witnessed in the last week, communication and first responder systems; and of course our defence capabilities, networks, and core elements.

The fact is that no industry vertical or sector is immune and we are now witnessing the evolution of a hybrid warfare. To provide the context of the narrative, hybrid warfare might be used informally to describe the ever-changing complexity and dynamics of the battlefield, which include the use of cyberwarfare as a precursor to a larger military action.

I will now discuss the attacks that occurred over the last several years on the power grid of Ukraine in 2015 and 2016, as well as in the Baltics back in 2015.

From a timeline perspective, first we will look at the malware used to provide an understanding of the tools utilized in these attacks. Secondly, the timeline will be explored, outlining how the attacks were carried out. Finally, this discussion will look forward, offering a viewpoint of the future of cyber-defence of critical infrastructure as it relates to irregular or as recently coined “hybrid warfare”, and the opportunities for both the Department of National Defence, NATO, and NORAD to enhance our response to this new type of threat.

First, in terms of the malware used in the attacks, typically when a prominent cyber-attack is discussed, there's usually a cursory description of the malware accompanied by a picture. You've all seen it. It's like the *Matrix*, the green screen superimposed on a black background, or a sinister-looking individual with their face covered asking you to send bitcoins. Things have now evolved.

You see in the news media reports for the technical descriptions to present a catchy narrative or story to keep the readers interested. However, it does not necessarily provide a full understanding of how the attack occurred. Conversely, taking a technical approach to understanding these attacks while providing a robust understanding of the attacks, often limits the audience. This in turn, however, restricts the ability of the work to explore the attacks in the larger picture or global landscape. As such, I hope to provide the committee with a balanced, middle-ground approach to explaining why and how the malware is functioning, without becoming overly technical. The last thing we all need to do is get bored with technical details.

The malware, dubbed BlackEnergy, which was reportedly used in the Ukraine attacks, is a Trojan, a program effectively hiding its malicious intent. It enters the system through a file distribution, through an email spear-phishing campaign. We've all received these types of emails, formerly referred to as a Nigerian email scam, asking us to wire money to specific African nations to secure the release of millions of dollars predicated on immediate action.

In the corporate and government realms, C-levels are constantly being targeted with requests to approve and authorize internal transfers of financials from their operation team, whether it's in general finance or procurement, to facilitate large money transfers to Asian banks, generally when they're about to go on vacation or head to the cottage. These types of campaigns are targeted. We call them whale-phishing campaigns. They appear as normal correspondence that the victims would experience in their day-to-day jobs, rather than a more generic one typical of a phishing campaign, which is treated almost like a numbers game.

Once that malware has been downloaded, it enables the attacker to launch a distributed-denial-of-service attack, as well as download custom spam and information theft plug-ins. In other words, once BlackEnergy had infected the systems in Ukraine, it was able to act as the gateway for the next stage of the attack, bringing in additional malware to allow for intelligence gathering and to facilitate those future attacks.

I wish to convey to this committee that there are multiple variants of these infections. These include BlackEnergy 2, which is a more precise tool used to go through specific systems, and BlackEnergy 3, which is focused on searching a network for specific or enticing systems, including those in government, military, and in overseas infrastructure. They seek to provide network reconnaissance and a mechanism to spread that infection.

The threat is present. This BlackEnergy malware then delivers a KillDisk into the system following the initial infection. This component of the attack made the systems within the infrastructure inoperable and gave the threat actor the potential to remove a central component of the infected systems, thus impeding restoration efforts. Once KillDisk is run, it wipes or overwrites all the key essential systems, including the master boot records, which brings down the systems and prevents a system reboot. This further hides the activity of the attacker within the system and disguises the effective nature and origin of the threat actor.

That's critical when you're determining who your threat actor is and basically, when you're doing your forensics, who you want to chase down if you're going to take a response and recovery measure.

● (1540)

Both BlackEnergy and KillDisk have been seen operating in conjunction with each other, and most notably in the Ukraine power grid attack in 2015. Current and future adversaries are likely to rely more on a blend of conventional and irregular approaches to conflicts, which has been referred to, as I mentioned, as hybrid warfare, and these may be a precursor to kinetic attacks.

In addition, another variant, the Industroyer, has been alleged as the malware behind the 2016 Ukrainian power grid attack. It's highly customizable with malware, and researchers believe it is targeting industrial control systems. If you look at the reports in recent weeks, effectively it's becoming more pervasive. It is a malicious tool in the hands of a dedicated, well-funded, and persistent attacker. This is not something that a script kiddie could take off the dark web and just implement.

The malware is able to persist in compromised networks and directly interferes with the critical working processes in those facilities. The malware is extremely dangerous. Its potential damage depends on the configuration of that particular facility, and can vary, for example, from one substation to another and can be anything from a simple local blackout through a cascading failure to potentially even greater damage to the hardware. The relatively low impacts of recent blackouts stand in great contrast to the technical detail, level, and sophistication of the suspected malware behind Industroyer. These threat-based actors are institutional at a government level.

A possible explanation for this, which is the opinion of many security researchers, is that this was a large-scale test. They're testing our perimeter defences, pushing the envelope, and observing our response and recovery methods. This is a calculated, strategic approach to hybrid warfare.

The security community in North America has compared Industroyer to the Stuxnet cyber-weapon, having formerly worked for Siemens, which was used to target the Iranian nuclear program.

I'm going to skip ahead of the time on the attack. I see the chair....

I will now provide a quick comment on how the power grid attacks unfolded, and the context of each attack.

Three attacks were examined: Ukraine, Baltics, and Ukraine. Before going into the individual attacks, it's important to note the attribution of these attacks.

First the available information only attributes the Ukraine attack to advance persistent threat Sandworm, which was believed to be a hacker group with the Russian government. In the 2015 Baltic attack, researchers claimed they saw evidence of Sandworm, but were unwilling to provide such evidence for operational reasons. This is part of the challenge that we're faced with in the industry in the response and recovery methods. The trust factor is key to a successful response. However, in many cases it takes months or even years to determine all the facts.

Finally, in the Ukraine attack the use of Industroyer had not yet been officially attributed to any country actor. Therefore, for the purposes of this section, the attack has been accepted by experts in the private sector as being launched by the Russians. Again only time and further due diligence will confirm this assessment.

I'm going to skip ahead from the attacks, because I think we've touched on it critically, and I'd like to focus on the prevailing attitudes.

The Chair: I'm really sorry. I'm going to have to stop you there. I'm hoping the rest of your testimony will come out with questions, but I'm going to have to yield the floor to Mr. Bell.

Mr. Alan W. Bell (President, Globe Risk International Inc.): Good afternoon, ladies and gentlemen. Thank you for inviting me here today.

Russia is becoming progressively more paranoid, as a considerable number of ex-Soviet bloc countries have applied for membership in either the EU or NATO. This is unnerving Russia, as it needs to maintain a strategic depth between the former Soviet bloc countries on its vast borders. It will need this battle space to be able to successfully manoeuvre in the event of a potential NATO attack or threat. Considering its history, Russia is not prepared to be invaded again.

When Russia illegally pushed into the Crimea, it utilized a hybrid warfare military strategy that blends conventional warfare, irregular warfare, and cyberwarfare simultaneously to achieve success. Through a combination of kinetic operations and harnessing other subversive efforts, the Russians attempted to avoid attribution and retribution.

In a practical application, the Russian concept of non-linear conflict exemplifies a typical hybrid war strategy. A non-linear war is fought when a state employs unusual, conventional, and irregular military forces in conjunction with psychological, economic, political, and cyber assaults. Hybrid warfare can be described as the use of flexible and complex dynamics of the battle space, which in turn requires a highly adaptable, well-trained, and resilient response. Unfortunately, neither the Ukraine military nor NATO was fully resilient to provide this response when this occurred.

Confusion and disorder ensue when weaponized information exacerbates the perception of insecurity within the population as political, social, and cultural identities are pitted against one another and plausible liability abounds. To use the Ukrainian conflict as an example, Russian hybrid tactics were used extensively during the annexation of Crimea. The subsequent civil war in eastern Ukraine caught the west totally off guard, particularly the U.S. and the U.K., who were unable to formulate any type of response.

NATO's inaction can at least be partially attributed to the rigid NATO military organization that it currently employs. More critically, Russian military and intelligence experts have accurately identified and exploited international legal frameworks governing the use of force against another sovereign state.

NATO military strategy, above all, must emphasize non-linear thinking in conflict modelling. The Canadian military, while aware of the use of hybrid warfare, is not trained to adopt non-linear thinking when they are undertaking conflict modelling and planning. To date there hasn't been any measurable western or NATO response to Russia's aggression in Crimea or Ukraine, other than providing political and economic assistance.

Unless the legal framework defining the act of aggression is reworked, other liberal democracies may be at risk. It seems increasingly clear that the primary method of ensuring continued rule of law is by overhauling our traditional interpretation of conflict. The west must develop a framework of strategic deterrents of weaponized information, finance, and other subversive forms of aggression. A one-size-fits-all policy will no longer be an effective deterrent in the future.

From the beginning of Russia's engagement in the hybrid war in Crimea, there was a profound emphasis on maintaining a degree of plausible deniability. The Russian flag was raised by residents of Crimea, not Russian soldiers. Russian forces were stripped of any identifying markers or insignia. Cyber-attacks were launched at Ukrainian critical infrastructure facilities and systems. These attacks were structured in a manner that attempted to obscure Russia's involvement.

Of course it's widely understood that Russia was responsible for the violation of Ukraine's sovereignty. However, the confusion that was spawned by the disinformation campaigns, cyber-attacks, unmarked Russian special forces, and later actions in eastern Ukraine would see the west committing further inaction by allowing the Russians to consolidate and then normalize the acquisition of Crimea by the Russian Federation.

Concepts of hybrid warfare are not taught at DND offices, which results in DND not being able to consider the manifestations of hybrid warfare when planning future military operations. Why is this?

● (1545)

It is because we do not utilize a whole-of-government approach, and neither do we fully explore these concepts, which include psychological, educational, economic, military, finance, political, legal, cyber, intelligence, and communications security. To my knowledge, apart from the U.S. military, no other NATO members' planning processes involve planning for hybrid warfare or linear conflicts.

How can we combat, train, and prepare for Russian active hybrid measures in the future, such as those currently being inflicted around the globe, if we do not understand how they work? This change now requires that the U.S. and its allies adopt a new legal, psychological, and strategic understanding of warfare and use of force, particularly by Russia.

In terms of options for Canadian international assistance in Ukraine and a UN peacekeeping mission in the Ukraine, numerous questions need to be asked before committing to any peacekeeping missions, for example, where and how to keep the peace, and how this can be achieved. Russia wants to be involved in any future peacekeeping mission. It will be impossible for Russia to be part of the peacekeeping mission, because Russia is on the side of the conflict as an aggressor.

What would a peacekeeping mission in eastern Ukraine look like? What are Operation Unifier's rules of engagement if they are attacked by hostile forces? Are there plans to deal with implanted Russian actors, both in the government and in the military?

Russia's veto on the Security Council would override a Ukraine-Canada peacekeeping ambition.

Contributing to a UN-led intervention in Ukraine and the troubled breakaway eastern districts, on the surface, might appeal to the current government as it would be in line with their method of the “Canada is now back” mantra, while at the same time fulfill the government's pledge to deliver 600 troops and 150 police officers to UN peacekeeping support operations overseas. There has been talk about a UN peacekeeping mission in the Ukraine since 2015, and so far, nothing has really happened.

In terms of our options, option one being to deploy UN peacekeepers, Russia might agree or not agree to a UN peacekeeping force in Ukraine. The Russians might demand to be part of it, and I don't know how that will be achieved. This peacekeeping mission could possibly be led by Canada; however, Russia might veto Canada as the lead mission as it could be seen as being too close to the U.S.

The discussion, organization, and deployment of a future UN peacekeeping force could take a considerable amount of time before deployment, somewhere between two to three years. At this time, Canada has agreed that a future mission would assist, while at the same time indicating that Canada has not yet decided where to commit the CAF in a peacekeeping role.

In terms of option two, what is required in training to provide full-spectrum military operations training to the Ukraine military? It is not just basic training and policing training, but more dynamic, full-spectrum training. The answer is to staff a command college to provide full-spectrum hybrid military operational training to Ukraine senior and junior military officers. There is a requirement to provide cyber-training and systems threat assessments to the Ukraine government, as well as the military.

A number of questions still need to be asked. What are the Canadian Armed Forces rules of engagement and resident capability to extricate those 200 Canadian troops if required to do so? If they are attacked, surrounded, or told to surrender, how does DND plan for another Russian offensive wave into the Ukraine? Has the CAF developed suitable evacuation plans to respond to all possible scenarios, and have these plans been tested? Is Canada prepared for an escalation in fighting, and what would be the ramifications to the military training teams currently in the Ukraine?

The rest of my presentation basically mirrors what my colleague mirrored, so I will not go that far. I will provide a complete breakdown of my presentation if anyone requires it to read later.

Thank you very much.

● (1550)

The Chair: Okay. Thank you very much.

Since this is your first time in front of the committee, my signal usually means, if you're in the process of responding to a question, you have 30 seconds left before I have to give the floor to the next speaker to make sure everyone gets their time.

Mr. Wright, I apologize for cutting you off. You are the most qualified person we've had in front of this committee with regard to cyber, so I'm hoping what you are going to say is drawn out by the questioning, because we know this is a very important aspect of what's happening over in Ukraine.

That said, I'm going to give the floor to Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Mr. Chair, thank you very much.

Gentlemen, thanks for being with us and for your expertise.

Mr. Chair, perhaps I can just take you up on the signal to allow Mr. Wright to briefly, in a minute or two, complete, maybe in bullet points, the remainder of his presentation. I think what he was saying was important.

Mr. Stuart Wright: I do apologize. My wife has always indicated to me that I'm long-winded, so I'll give you the call to action, the bottom line here.

My recommendation is, first, revise and adapt the existing Department of National Defence's official doctrine to provide more prescriptive details on how the DND and its strategic partners, including NATO, might incorporate military approaches to warfare, including cyber.

Second, provide and adopt a handbook for how to adaptively counter the countermeasures, and establish a mechanism to share these response and recovery tool kits only with trusted partners, including what my colleague had indicated with that fusion centre concept.

Third, consider adopting a community or practice guideline or framework to enhance response and recovery measures, as it is likely that we are to be hit, and with ever-increasing attacks, our resilience and our flexibility to respond will need to be honed.

Fourth, adopt appropriate measures, including tools, techniques, and people—TTP—to support the above-mentioned efforts.

Finally, continually test and adapt response measures and ensure operational capabilities both abroad and domestically.

● (1555)

Mr. Sven Spengemann: Thank you very much for that.

Mr. Wright, to put this into a broader context, of all the problems that the current government has in the Donbass region, could you give us an appreciation of how big a problem the malware and cyber-attacks are? Are there any non-cyber-backstops, any immunizations, other than counter-attacks or cyber-based defence mechanisms, that the current Government of Ukraine could put into place to immunize or protect itself?

Mr. Stuart Wright: If you look at recent incidents in the United States with the Equifax attacks or other incidents like the Dyn attack, which paralyzed the east coast's Internet security measures, you see that you have best-of-breed industry best practices currently being utilized here in North America. We should be leveraging those toolsets, knowledge, and learnings, and applying those in the remote jurisdictions, including in Ukraine.

The defence and depth measure and approach that they've currently adopted to protect their critical infrastructure is good. We need to start thinking in terms of response and recovery. We know we're going to get hit. We know the sophistication of the attacks. They're going to keep cascading and escalating up. We need to be able to work with Ukraine to basically provide current-level threat intelligence and respond appropriately with appropriate tactical teams.

Mr. Sven Spengemann: The two attacks you described, in 2015 and 2016, are they the most significant, the largest, the most complex attacks that NATO has ever faced on the operational side?

Mr. Stuart Wright: To date. Again, these are the ones that have been reported in the Ukraine and eastern Europe. From our understanding, these are the ones that were widespread. They were able to disrupt the operations and take down the grid, and it took a significant level of effort to restore the power and critical infrastructure.

What we're seeing here is that they're testing the perimeter. They're determining how we're responding. They're looking at this not as a mechanism to take down the grid for a larger effort. They're testing how quickly we can respond, who we're bringing to task, and the measures and mechanisms. We need to start looking at this from a strategic perspective. They're testing the perimeter right now. We haven't been fully hit.

Mr. Sven Spengemann: Thanks very much, Mr. Wright.

I'm going to move away from the cyber side. I'm sure colleagues will have follow-up questions on that front.

Mr. Stuart Wright: Sure.

Mr. Sven Spengemann: Mr. Bell, very briefly, can you sketch for us what Globe Risk International does?

Mr. Alan W. Bell: We're an international security consulting company, and most of our work is done in hostile countries around the world.

Mr. Sven Spengemann: Geographically, you have expertise in which areas?

Mr. Alan W. Bell: I spent 23 years in the British Special Forces. I immigrated to Canada and I've had my company going now for 21 years.

Mr. Sven Spengemann: Thanks very much for that. I'm going to ask you some questions.

Mr. Siromakha, welcome to the committee, and feel free to jump in on these questions as well.

Colonel Viktor Siromakha (Defense, Naval and Air Attaché, Embassy of Ukraine): Thank you very much.

Mr. Sven Spengemann: Mr. Bell, you spoke of the peacekeeping mission. Do you see a political pathway into a UN-led peacekeeping mission in the Donbass region without Russian acquiescence or support or approval?

Mr. Alan W. Bell: I think it will be difficult to achieve without Russia's consent because they hold veto powers at the UN and they can really dictate what they want to do. They could force themselves into that mission in whatever way they wanted to portray themselves, and I don't see how the UN can stop them from doing that.

Mr. Sven Spengemann: Do you see a political pathway possible with potential Russian participation?

Mr. Alan W. Bell: Yes. It's going to be difficult because we don't know what the Russians' intentions are. They stopped in the Donbass region. At this time next week they could be somewhere else. We don't know what they're going to do. The fact that NATO was inactive and didn't really stop them from doing that and didn't really hold them to account for it will probably ensure that they get more and more adventurous in their actions. The other former Soviet bloc countries on their border are also worried that they could be next, and that this could be the first of many incursions into their countries as well.

Mr. Sven Spengemann: The committee had testimony from Ambassador Waschuk, who suggested the price for Putin, with respect to retaining control of the Donbass region or at least occupying it, is going up. Do you agree with that?

Mr. Alan W. Bell: Yes.

Mr. Sven Spengemann: What might be the key factors in elevating that price?

Mr. Alan W. Bell: Every day we—the west and NATO, I'll just combine the two—do nothing except on the political levels, which probably none of us will ever know about at that particular time, they are getting more and more adventurous, and they will do more and more. They have the power to do that. The whole Russian army's aim is to fight a war on land on their borders, and that's what they are geared up to do. Of course, all the other former Soviet bloc countries are not able to defend themselves against those types of attacks.

● (1600)

Mr. Sven Spengemann: Is it a smart question to ask whether Mr. Putin has an end game in the Donbass region, or do you think he may not even know what his end game is at this point?

Mr. Alan W. Bell: I think he is testing the water. The only thing I can see changing is if he comes out of power and someone else takes over who is a little easier to deal with. That doesn't seem to be on the horizon at this particular moment in time. The less we do to stop him from doing it, the more he will probably plan to escalate.

Mr. Sven Spengemann: Thank you, Mr. Bell.

Mr. Siromakha, I'd like to ask you for your answer to that same question, recognizing that I am almost out of time, so colleagues will probably follow up with you. How do you see Mr. Putin's end game in Donbass? Is there one? What do you think is next?

Col Viktor Siromakha: I think the dream of Mr. Putin is to create something similar to the Soviet Union. For him, as quite an aged and experienced man, that would probably be the masterpiece of his whole life. He is probably trying to finalize his tour of duty as President of Russia with a very big and serious step, creating something very big and really strong.

Mr. Sven Spengemann: Mr. Chair, I think that's my time. Thank you.

The Chair: Thank you.

Colonel, thank you for joining us. I'd like to bring you into the conversation formally. I'll give you your 10 minutes, for your opening remarks, and then I'll resume questioning with Mr. Hoback.

Colonel, you have the floor.

Col Viktor Siromakha: Thank you very much, sir.

Honourable chair of the committee, members of Parliament, ladies and gentlemen, I'm grateful to you for giving me this opportunity to represent our Ukrainian understanding of the ongoing conflict in eastern Ukraine.

Has something changed in Russian deeds and behaviour in the last three years of war? Nothing. Let me reassure you that people are still dying in the conflict every single day. Yesterday was another dark day for Ukraine. We lost four Ukrainian soldiers, killed in action. Four other soldiers were wounded. Just think: four women woke up as widows, children lost their fathers, and mothers lost their sons. Ukraine strives for peace, as I believe everyone in this room does, but today we are still forced to keep searching for a response to Russian aggression.

The aim of Russian aggression is to destroy democracy, liberal freedoms, and human rights in Ukraine. In some places they do this with tanks, in other places with the help of fake news, hybrid warfare, including cyber-tools, like yesterday. They assaulted the Ukrainian airport at Odessa and the Kiev subway system, so it was one more bright example of their cyber-tools.

Russia keeps blatantly violating the commitment taken upon itself, the same way Moscow keeps ignoring our persistent demands, and demands of the international community, to get back to respect the international floor, but Russia keeps pretending it has nothing to do with that. Moscow continues to turn a blind eye to its commitments under the Minsk agreement. Its military forces are still on the territory of Ukraine, both in Crimea and Donbass.

Let me dwell upon the current situation in eastern Ukraine. The conflict-affected areas of Donbass have suffered enormous losses. More than 10,000 people were killed, more than 20,000 people injured, and 1.5 million were displaced. Bridges, roads, houses, and other infrastructure elements were destroyed. Huge terrains are now polluted with anti-personnel and anti-tank mines, and booby-trapped mines as well. Many plants and factories were stolen and the unique equipment was illegally transported to Russia. Military assets, weapons, ammunition, fuel, and rations are still delivered to illegal entities created by Russia. The security situation remains very difficult.

Combined Russian separatist forces continue to systematically ignore the Minsk agreement, making extensive use of the prohibited weapons. The vast majority of armed provocations are carried out in the dark, after the OSCE and the Red Cross finalize their daily missions. Mercy observers have no unlimited access to the areas not controlled by the Ukrainian government, which does not allow them to really assess the status of the implementation of the Minsk agreement, like in the vicinity of the village of Telmanove two days ago—just two days ago.

On the other hand, on numerous occasions Ukraine proved its readiness for a peaceful settlement of the situation that was artificially created by Russia. In 2017, Ukraine has initiated long-lasting ceasefires three times: Easter, harvest, and so-called back-to-school ceasefires. Russian occupation troops and their proxies violated them almost straight away. Since the beginning of 2017, there were more than 13,000 registered violations of the ceasefire regime. Several weeks ago, the Ukrainian parliament adopted a law establishing conditions for a peaceful settlement in certain areas of the Donetsk and Lugansk regions. They count on Russia finally beginning to implement security commitments under the Minsk agreement. We also expect that these steps will allow moving forward with the matter of the deployment of a UN peacekeeping mission in Donbass.

The initiative of this peacekeeping mission was introduced by our president in spring 2015 to the UN Security Council. Ukrainian delegations to the UN have continuously requested sending an assessment mission of the UN Security Council to Ukraine to study the situation in the field. Unfortunately, all proposals faced a rigorous opposition on behalf of the Russian delegation in New York, which argued that such an operation would be in contradiction of the Minsk agreement.

● (1605)

The Ukrainian side is ready for constructive work under the deployment of a full-fledged UN peacekeeping mission. However, the project suggested by Russia cannot serve as a basis for a pre-review discussion within the Security Council.

The principle elements of the Ukrainian position are the following.

A future UN mission should be deployed throughout all the temporarily occupied territory, including the uncontrolled section of the Ukrainian-Russian state border. The introduction of a UN mission should immediately lead to a steady ceasefire, as well as to a complete withdrawal of all foreign troops, armoured formations, and personnel, including their weapons and equipment, from the territory of Ukraine.

A UN mission should comply with the guiding principles of the implementation of UN peacekeeping operations, which exclude the participation of representatives of the aggressor country or other parties to the conflict. Therefore, Ukraine rejects coordinating the future parameters of a UN mission with pro-Russian separatists. A future UN mission should not in any way harm the OSCE or other international organizations in Donbass by preventing them from fulfilling their mandate or restricting their freedom of movement.

Ladies and gentlemen, let me once again answer my own question. Has something changed over the last three years since the beginning of the war in Ukraine? Yes, it has. The international coalition in support of Ukraine and the rule of international law has only strengthened. I'm very pleased to stress that Canada has been one of our main partners and friends in supporting Ukraine's sovereignty and territorial integrity.

This year we celebrated the 25th anniversary of the establishment of diplomatic relations between Canada and Ukraine. Ukraine is totally committed to the continued deepening of bilateral relations. Canada and Ukraine continue to work together on military training and defence matters.

In April of this year, Canada and Ukraine signed a defence co-operation arrangement, which shows Canada's steadfast commitment to Ukraine and the Ukrainian people. Throughout Operation Unifier, the Canadian Armed Forces delivered more than 160 courses to 5,800 Ukrainian soldiers. This year, for the sixth time, a contingent of approximately 30 Canadian Armed Forces members deployed within Operation Unifier marched in the Ukrainian independence day parade.

We are grateful to the Canadian government for extending the mandate of Operation Unifier until March 2019. We are looking forward to the positive decision of the Canadian government concerning adding Ukraine to the automatic firearms country control list. The initiative is vital. Let me stress this one more time; it's vital for Ukraine. Yes, Ukraine does need defensive lethal weapons as a country entering the fourth year of a very real and brutal war.

Ukraine highly appreciates the political support and essential practical assistance of the government and people of Canada provided to the Ukraine armed forces. I am very grateful to the honourable members of this assembly for protecting Ukraine from the Russian aggression from the very beginning. The people of Ukraine will always remember the hand of support extended to us by our friends in the most difficult moment of our history.

Thank you for your attention, support, and confidence.

Glory to Ukraine. Glory to Canada.

● (1610)

The Chair: We offer our sincere condolences to you for your soldiers lost yesterday in the fight with Russia.

Col Viktor Siromakha: Thank you very much.

The Chair: Mr. Hoback.

Mr. Randy Hoback (Prince Albert, CPC): Thank you, Chair.

Thank you to all three witnesses for being here this afternoon for this great discussion.

Cybersecurity, fake news, cyber-hybrid war—all that seems to be in Ukraine, and it seems like it's one of the fronts for that to happen. It seems like it's where all the new stuff is being developed or tested, if not utilized. We saw that, as you said, last night.

How does the "cyber" aspect redefine war? How does it change what we should be doing in Canada as far as preparing for our own protection? Also, how can we assist people in Ukraine similarly to what the Americans and the Brits are doing in helping to provide that cyber-technology, that cyber-assistance?

Mr. Bell, I'll start with you, and then Mr. Wright.

Mr. Alan W. Bell: Warfare has been the way it's been for many years. This is a new spinoff from actual war and what we're used to planning for and what our leaders are used to dealing with over time. These forays into these different countries, we get them in Canada but it doesn't mean to say we're going to get invaded. However, in the Ukraine and in Crimea, they were preconceived attacks that resulted in annexation for Crimea, and then some occupation of the Ukraine.

We did not know or we didn't realize at the time that this is what the cyber-attacks were a result of. Of course, the other countries in that part of the world are going to be worried that if they start having more and more cyber-attacks against their particular critical infrastructure facilities, Russia is going to make a move into their country.

This is what worries them. It should worry us as well because we have to deal with them as well, as well as most of the other western countries. Until we really get a handle on cyberwarfare—and I think my colleague wants to talk about quantum computers shortly, which could be a deal-breaker for all this because I can't talk about that type of thing—I think we're going to ask, when we have this overabundance of cyber-activity, what does it mean? Does it mean they're just feeling us out, or does it mean this is a precursor for another attack?

Mr. Randy Hoback: In this case, they used the precursor for an actual attack.

Back in North America that could be a precursor for an election or some other activity that disrupts the media, disrupts the flow of Canadians.

Mr. Wright, how do you see all this linked together? What could we be doing in Ukraine that would help us prepare here in Canada? For example, the attacks that happened yesterday, if we were there, what would we learn from it that we could take back to Canada? Because we're not there, we don't learn.

Mr. Stuart Wright: Immediately, you threaten intelligence. We'd understand the boots-on-the-ground view as to what the threat actor was doing, how it orchestrated the attacks, the tools and mechanisms that are used to deploy those attacks, which critical infrastructure, why it was targeted at the time. I'm hearing of casualties. It sounds as if this was a concerted effort, timed strategically so that there might have been a frictional escalation at the same time.

To go back to your initial question of what we can do domestically and abroad, first you want to improve the domestic cyber-capabilities, both in Ukraine as well as here in North America. Given the repeated expectation of vulnerabilities in industrial controls like SCADA systems, which took down the air systems and the transport automation systems, we want to focus on that in industry, government, and the military.

Some questions were raised here by the panel. My comment would be training exercises as well, like NATO's locked shields, are an excellent means of reducing the impact. It doesn't address the latent vulnerabilities found with these industrial systems, so we need to start training, mobilizing, and resourcing to address the current risks there. For example, as part of the exercises, NATO members defended the power grid in Estonia from an ongoing cyber-attack.

Such a defence, while essential, needs to be accompanied by proactive measures such as updating and improving industrial system security. Otherwise, all these are just workarounds for active defence measures. They're going to keep implementing new tools, new malwares. You need to start hardening these systems. You need to have people on the ground to assist Ukraine, take those learnings, and bring them back to North America.

● (1615)

Mr. Randy Hoback: That begs the question. Here in Canada we have a conventional idea of military being guns and soldiers. Do we need to redefine military and war?

Mr. Stuart Wright: As part of that playbook we need to redefine hybrid warfare. We know we can go kinetic. We have the tools, processes. We have some subject-matter experts here that I could learn from on how to go kinetic. You need to understand as a precursor to those activities that cyberwarfare is the first mechanism for effectively disrupting your communications, disrupting your measures for energy, which causes chaos in your systems and impacts your ability to respond kinetically. If you're going to go down that path, you need to start resourcing up, training up, and providing additional tools, processes, and measures to help support the troops in these foreign operations both here and abroad.

Mr. Randy Hoback: Okay, so Mr. Bell, in that case, you don't necessarily want people who can do 100 push-ups. You want people who are like Sheldon Cooper of *The Big Bang Theory*. How do we attract those kinds of people?

Mr. Alan W. Bell: We need to redefine the battle space, and that's why I'm talking about military advancements.

I'd like to go offline a minute. We're responsible for carrying out an extensive audit of one of the province's water supply systems. All our SCADA systems were not protected in any shape or form. I asked the individuals in charge of this water supply system, what would happen if they got cyber-attacked? They said, people in that particular province would not have water for a minimum of about one to two months.

Imagine if that happened in the summer and we lost the ability to deliver water to a province. I'm not talking about a city. I'm talking about a province. This province would have been totally vulnerable. They still haven't figured out how they're going to protect them.

Mr. Randy Hoback: In other words, we would be vulnerable not just in power grids—

Mr. Alan W. Bell: We are vulnerable now, today.

Mr. Randy Hoback: —but in water and a variety of other things that we probably can't even imagine.

Mr. Alan W. Bell: Yes. I'm not even going to go on to our nuclear power stations.

Mr. Randy Hoback: Back in Saskatchewan, the malware that was used yesterday could actually show up on Saskatchewan's power grid or something like that. Is that fair to say?

How do we defend against that?

The Chair: You have about 20 seconds, so you can respond.

Mr. Alan W. Bell: Do you want to answer that question?

Mr. Stuart Wright: I'll answer that question.

We need to develop a framework, come up with a common knowledge and approach, and start training resources now, because the threat is escalating. It's evolving every day, and new tools are coming out. If we don't have a common framework to protect all critical infrastructure, then we are basically operating from a dark position.

Mr. Randy Hoback: Thanks, guys.

The Chair: Ms. Hardcastle, welcome. You have the floor.

Ms. Cheryl Hardcastle (Windsor—Tecumseh, NDP): Thank you, Mr. Chair. It's good to be here.

I am really intrigued by everything that you gentlemen have offered.

Mr. Wright, I want to go back to you. From what you've been talking about, the question of Canada and our next steps.... Do you believe that, in order for us to harden our systems, whether it's a province or a municipality with water supply or a power grid, the onus for the framework you were talking about, developing a strategy, should be on some national entity, maybe in the Department of Defence, which would be approving or screening these new infrastructure grids?

From what I am hearing and from what I've understood from my reading, we are beyond using the metaphor of the firewall. It's almost like we need to be using some kind of metaphor that's similar to the way we construct buildings in earthquake-prone areas. We have to have these self-contained structures.

How do we have a master strategy? I just wanted to hear more. I think you were cut off a bit, so I'll use up the rest of my time with that and let you freestyle.

Mr. Stuart Wright: There are a number of different measures and mechanisms we can take. The framework.... Again, I have to tread very carefully here. I am speaking as an individual, and I'll caveat my statements.

It would behoove Parliament to consider a federated model to adopt a framework not just for the Department of Defence but for all critical infrastructure providers uniformly across this country, whether it's transport automation, waste-water management, or the financial service sectors. There are precedents here: in Australia, Italy, and other jurisdictions. I know the United Kingdom and Germany looked at this.

My guidance would be to take the core elements that we've seen out there, like NIST and the Department of Energy's C2M2, with the mil-spec, and incorporate two additional elements. One would be security by design; for every item and mechanism we are putting into place, fundamentally incorporate that into the actual development as part of our infrastructure build-out and our measures build-out. The second one, respecting the fact that we live in a democratic society, would be privacy by design. I think of Ann Cavoukian here. We should be espousing that with leaps and bounds. This wouldn't be specific just to the energy sector. It would be specific to all our sectors.

We need to look at this holistically. We need to work with our provincial partners inter-jurisdictionally, both here in North America and abroad, to respond collectively as a sector. Collectively, we are stronger. Individually, we are weak. We need to think federally, and we need to think beyond our borders. We need to engage with our partners abroad, with NATO and our counterparts in Ukraine, to basically come up with a mechanism such that we can speak the same language, respond in the same time and fashion, and have the same types of resources and training, so that if we need to deploy to a certain theatre of operations, we have the resources available, both in industry and in defence, to actually respond.

I won't speak about quantum computing right now, because I don't want to terrify anybody.

● (1620)

Ms. Cheryl Hardcastle: I have a little more time.

You had an example earlier. You were kind of cut off in your presentation. Do you want to go back and talk to us a bit about some of the examples that prompted you to tell us that we need a federal plan that goes beyond our borders?

Mr. Stuart Wright: We were cut off around the Baltic attack. Around the same time was the 2015 Ukraine attack. One of the three Baltic states—Estonia, Latvia, and Lithuania—saw its power grid attacked, but it wasn't taken down. The exact country that was attacked had not been announced publicly. The attack on the Baltics followed a similar methodology as in Ukraine.

What we are seeing here is that they are using the same playbook to disrupt different jurisdictions, but we need to respond not just individually but collectively: a federated model, a federated framework based on industry practices. I know that Google, Apple, the Department of Defence, and Homeland Security are all standardizing on NIST as a solid framework. We've had a lot of conversations along those lines. Separately, I can share with you what we are doing here in Ontario.

Overall, that attack was largely unsuccessful, but it did expose one thing: the actors' presence in the Baltic power grid. They may already be in the power grid systems, and they may have already deployed that malware. What we need to do is take the appropriate measures to validate that these systems haven't already been compromised.

For us to do so, we need to have the resources and the training, and we need to start hardening those systems. If we want to replicate it—whether it's in Estonia, Ukraine, or here in Canada—we need to speak a common language. That framework would be the foundational element that is required. My recommendation to this panel is to start considering that, and adopting it as a measure.

Ms. Cheryl Hardcastle: Thank you.

The Chair: Mr. Robillard.

Mr. Yves Robillard (Marc-Aurèle-Fortin, Lib.): Thank you, Mr. Chairman.

[*Translation*]

Good afternoon gentlemen.

Thank you for your input today.

Mr. Bell, I'm going to quote from your bio.

[*English*]

Mr. Bell has trained close protection teams for two kings, two presidents, and has been involved in countering terrorism operations and training throughout the world.

Mr. Alan W. Bell: Yes. I have done that.

[*Translation*]

Mr. Yves Robillard: Given your expertise, what can you tell us about the security risks the current leaders of the Ukrainian government face?

● (1625)

[*English*]

Mr. Alan W. Bell: The main risk is Russia going one step further. In other words, what the Ukraine is worried about, as well as the other former Soviet Union bloc countries, is the fact that Russia is going to take back more areas within those countries, to enable it to have a bigger operating battle space if NATO decides to attack.

There is very little chance that NATO will attack, obviously, the way things are at the moment, but NATO did agree—I can't remember how many years ago—that they would not increase the size of NATO using other countries in Europe, but in fact, they've gone to 29 countries that are now involved with NATO.

Obviously, as I stated in my presentation, Russia is getting very paranoiac. They're not only worried about Europe. They're also worried about the Turks. That's another issue, because the Turks have indicated that whilst they are a member of NATO they also want to try to become the leader of the Muslim world, and those two ideas aren't computing.

Also the Black Sea fleet.... If NATO decides to stop the fleet from coming through the Bosporus and Dardanelles, that fleet is no longer able to operate in a warm water. The only port they now have is Tartus, in Syria. That's the reason why they're engaged in Syria.

[*Translation*]

Mr. Yves Robillard: Are private security forces increasingly playing a role in the conflict in Ukraine? Is that a trend you're seeing?

More broadly speaking, how involved is the private sector in the conflict in Ukraine and its most dangerous areas?

[*English*]

Mr. Alan W. Bell: There have been a lot of private military corporations, mainly U.S. private corporations, that have gone in. They are assisting the Ukrainians with various different training and how to operate, especially in urban areas where a lot of these battles are taking place.

In terms of how many companies and what their strengths are, we do not know at this particular moment, but they are starting to move in there. That's why PMCs were actually put together to go in and assist these countries when these countries didn't have a lot of help from outside their country.

[*Translation*]

Mr. Yves Robillard: Given what you know and what you've seen, what condition is the border between Ukraine and Russia in? Is it porous, and, if so, in what way? How great are the security risks in that area?

[*English*]

Mr. Alan W. Bell: Ukraine is facing a very fast, mobile, highly equipped and trained army. While Russia has not gone any further than Donbass at this particular time, who knows what's going to happen?

The cyber-attacks are getting more and more intense, and that's for one or two reasons. They're either trying to ensure they have it right the first time, or they're just seeing what happens, what the response is. The responses from the west, and NATO in particular, have been negligible at this time and this has emboldened them to do more and more. Consequently, until some type of peacekeeping force is put into place, Ukraine is going to be in constant fear of there being a total invasion or an annexation again, as happened in Crimea.

[*Translation*]

Mr. Yves Robillard: What do you make of the tactics being used by pro-Russian separatist groups against Ukrainian armed forces in the Donbass? How has Russia's support for separatist groups in the Donbass changed since the conflict began? What type of support has Russia provided?

[*English*]

Mr. Alan W. Bell: Russia is providing assistance right across the board. A lot of the pro-Russian side is actually Russian special forces. The media call them the green men. They are all over the place. They have a huge special forces capability in Russia, and that is now filtering over the border at various times to assist, train, and actually operate on behalf of the separatists within the Ukraine. This is something that's very difficult for the Ukrainian governments, and in particular the Ukrainian military, to be able to deal with because of the simple fact that they don't know who these people are because they all speak the same language. If you take a uniform off of a special forces soldier, he can be anybody.

The Chair: We're going to move to five-minute questions now.

The first five-minute question will go to Ms. Young.

Ms. Kate Young (London West, Lib.): Thank you very much.

Thank you, gentlemen, for being here today.

I want to pick up a bit of the conversation with talking about Russia pushing the envelope and watching our response. I'm trying to get a sense of what the west needs to do or what we need to do to make sure they back off. What is it specifically? Working together is one thing, but what do we need to do to show them that they can't continue with these cyber-attacks?

● (1630)

Mr. Alan W. Bell: We have to be committed. The country that's been attacked is Ukraine. We have to show commitment from the outside that we're willing to protect and go to the next level with Ukraine. If we don't, Russia will start looking at all the Baltic states, and then that becomes a bigger issue. All they're trying to do, from a Russian perspective, is to buy themselves some time, and in between that time is a country. They have to either have a foothold in that country or they have to annex that country.

That's what all the other countries are worried about. If you speak to anybody all through to the west of the Ukraine, they all think the same thing. All these countries have had their own meetings, and they've had collective meetings, and they are saying, “We're worried. What are we going to do?” Until NATO or the west or the U.S. decide on what they're going to do, they don't really know what to expect.

The problem they also have is that the leader of the free world, President Trump, has his eyes on other parts of the world and not particularly on Europe at this moment in time. They're worried about that. If there had been another president in the White House, maybe they wouldn't be as worried, but at the moment they are worried about what is going to transpire in the weeks and months ahead.

Ms. Kate Young: Go ahead, Mr. Wright.

Mr. Stuart Wright: I concur with Alan. He can speak better to the geopolitical elements here.

My concern here is in antagonizing the Russians. I know part of the friction points that we're seeing in the Baltics and in Ukraine is the fact that they're doing a transition from the BRELL grid to the European network. We're creating perimeters now between these two regions. There's a high degree of uncertainty about where the attacks are coming from, the attribution.

Let's be clear here. We have a hostile actor clearly in open warfare through either direct or indirect means. The challenge from a cyber perspective is how you go about saying, yes, it was Russia that was attacking and bringing down the grid. It currently happens to have military forces running in parallel. It seems like an awful coincidence if it wasn't.

From my perspective, you need to come up with mechanisms to verifiably attribute that. To do so, you need to have the resources and the will. In the United States we're seeing that they have an emphasis. They're focusing in other areas, this discussion about trade practices and whatnot. Again, if this is going to continue and if NATO wants to take a more measured approach, in addition to the appropriate level of forces, they need to factor in that cyber is part of that hybrid warfare, such as having trained resources to help with deployment and trained resources with the response and recovery for the industrial systems and whatnot.

Ms. Kate Young: Colonel, did you want to add to that?

Col Viktor Siromakha: Yes. I would like to add that in the beginning of 2014, when Russia illegally annexed Crimea, it was only the first step in the further development of the situation by military means. The essential question for them was to get ground corridor transportation to Crimea throughout the Ukrainian territory. That's why in July-August 2014, they have been doing their very best to get control over our southern city, Mariupol, and there was heavy friction between the pro-Russian forces and the regular forces of Ukraine, the ministry of the interior, and special security services. We've managed to protect Mariupol from their assault. Nevertheless, they've been using even MLRS to destroy some objects in Mariupol.

As far as I remember, some of the worst-case scenarios from British experts were whether Russia would get control over southeastern Ukraine, including Odessa, and a direct corridor to Transnistria, or we could get control over the left bank of Ukraine. You know probably that the territory of Ukraine is divided in two by our main river, the Dnieper. The worst worst-case scenario was, if they could get control over 70% of the Ukraine, then only a few regions on the west would be Ukrainians at least, so Lviv, Ternopil, Rivne, all these regions. As far as I understand, they didn't manage to do it, so now they're using both tanks and hybrids in order to get their goals.

● (1635)

Ms. Kate Young: Thank you very much.

The Chair: Go ahead, Mr. Yurdiga.

Mr. David Yurdiga (Fort McMurray—Cold Lake, CPC): Thank you, Mr. Chair.

My first question is to Mr. Wright.

We're very concerned with cybersecurity. With our own systems, we all experience some sort of malware. I assume that every system in Ukraine has been compromised at some level. Realistically, how long would it take to bring the systems up to date where we're comfortable that they won't be compromised? It's a hard question to answer because we don't know what has to be done. I'd just like your opinion on that.

Mr. Stuart Wright: That is the 10,000-mile view question. It's a significant question to ask. We're struggling with it within our own critical infrastructure and the fact that you need to have effective asset management. First, what are the assets in the field that you need to update? Second, are they vulnerable? Third, do patches currently exist and how are you going about updating those patches?

With the computers we have in our home and the laptops we have in our offices, you'll get the updated patch. It'll be pushed. There's a mechanism and an ecosystem that helps support that. With SCADA systems, sometimes you actually have to take them offline to harden these systems, so there is no real measure that you can actually bring to that. How do you determine that, if you don't know what assets you have, and identify whether that manufacturer has a patch in place to actually remediate? It would be very difficult at this junction to give you an assessment as to how long it will take them to harden their systems or update them to the vulnerabilities we know.

The concern that we should have is the unknown unknown vulnerabilities? We need to come up with a measure with the knowledge that these systems are likely to go down. What steps are you going to take once they do go down? What is the response and recovery? Then once you bring them back up, harden them at that junction. We need to take a different tack. You take a preventative measure and then a reactionary measure. We're already in reactionary. When you're in conflict and you're in the field of operations, how do you go about addressing that while you're in the middle of a battle conflict?

How can you bring your electricity grid back up and get your engineers out to make the system safe while there are shells falling around and casualties being taken? It's a very difficult assessment to make.

Mr. David Yurdiga: Is it fair to say that there's a plan being formulated? Obviously, this is a big task. We're looking at years and not months—

Mr. Stuart Wright: I would concur, yes.

Mr. David Yurdiga: —so we continue to be at risk. All nations are, actually. Ukraine is the test area. Do you foresee Russia expanding its cyber-attacks on its neighbours?

Mr. Stuart Wright: Here's the challenge. Again, it comes back to attribution. We know that in certain interests.... Alan had mentioned Turkey and we had also spoken to Ukraine and eastern Europe. We know that there are very strong indications that Russia is active in those theatres of operation. The concern we have is, what about third-party attacks?

We know that we've seen attacks come out of other countries, like India. I believe that there have been attributions out recently, with Thailand and the Sony attacks as examples. We've also heard about attacks originating in Africa. Are these nation-states going to war and using cyber-mechanisms to attack other nation-states or are they being used as third-party entities? How do you go about doing a forensic analysis? How do you trace back to the actual threat actor? That's the challenge. There's no clear-cut assessment.

If you had asked me whether we got hit by the Russians, we're seeing indications coming out of eastern Europe or out of Estonia. It may be a cyber-gang. It may be a third-party entity. It may be other threat actors from other regions. It may be China. It may be folks in Latin America. We don't have a coherent mechanism to determine those threat origins or to be able to map them back in a respective time. We need to have that ability. We need to get the actionable intelligence.

Mr. David Yurdiga: I guess the question for everyone is the cost. Are we putting enough money toward this issue? Obviously it's a concern for everyone. Do you think the governments are doing enough to put money toward securing our systems?

Mr. Stuart Wright: I have to tread very carefully here. Which government are you referring to?

Mr. David Yurdiga: Obviously, with everybody involved in a conflict.... Canada, for instance—

Mr. Stuart Wright: In the federal government...?

Mr. David Yurdiga: Yes, and also all the players. Obviously we're concerned about Ukraine. Are we giving enough funding for Ukraine to stabilize their systems?

● (1640)

Mr. Stuart Wright: The chair has indicated a 30-second flag. I'll be very quick.

More measures are requiring additional resources. That would include additional dollars. You need to ramp up your resources, which means that you need to start hiring specialists in this area or training up those specialists. More needs to be done. More dollars need to be expended in these efforts.

The Chair: Mr. Fisher.

Mr. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Thank you, Mr. Chair.

Thank you, gentlemen, for being here, for your expertise, and for your testimony.

One of the things about being near the end of our study and your being the last panel is that so many of the questions have already been asked, but I'm fascinated by the cyber side, as all of us are.

Mr. Wright, you're talking about this new type of warfare. You mentioned Bad Rabbit malware, KillDisk, BlackEnergy. It sounds like a whole bunch of energy drinks.

Mr. Stuart Wright: The effective product marketing is there. You already have the captive audience. That's actually quite brilliant.

Mr. Darren Fisher: Are there any instances of this cyberwarfare that are absolutely traceable right back to Russia?

There's an assumption. I agree with the assumption. I think we pretty much know exactly what's happening, but they won't even really admit to having soldiers in what they sell as a civil war area. Has there been an instance where we can legitimately trace it back, put a finger on it, and accuse them, rather than just what we assume?

Mr. Stuart Wright: I'm going to be careful because we're not convening in camera. There are security levels that are required for me to discuss in open context that question.

I will say the following. If you look at the December 27 Department of Homeland Security-FBI JAR report, which provided specific details to Russia's involvement with the electoral process south of the border, which was spoken to earlier, that is direct evidence of the capability, sophistication, and pervasiveness of the Russian cyber-threat.

From a hybrid solution in these other jurisdictions, I can go back and we can revisit this, but we have a pretty clear indication of attribution in Russia in at least two or three of those arenas, one specifically with Sandworm, with the Ukraine outages that we saw in 2014 and 2016.

Again, there is some concern. In Estonia, I believe, they did not want to come and say outright that there was an attribution there. We're not sharing that information, which is unfortunate. It's hard to make that determination.

Mr. Darren Fisher: With recent issues such as subways shutting down and airports shutting down, we are just.... There's an assumption there, but....

Mr. Stuart Wright: That happened on Tuesday. We got word of it, I guess.... The notifications went out Tuesday night when I was flying in.

Again, they need to have boots on the ground to look at the forensics, but early indicators are suggesting a very strong leaning that when you're doing this full theatre conflict and then you're shutting down the ability to transport troops, taking down power grids, disrupting airlines.... It's a very unusual coincidence, I would say.

Mr. Darren Fisher: Thank you.

Colonel, thank you for being here.

You mentioned in your opening remarks that you feel Putin sees this as his legacy. To rebuild the former Soviet Union is.... I don't know if you said “pièce de résistance” but it's his legacy, what he wants seen as what he left behind. So many people are suggesting that the aggression of Russia is because of Ukrainian interest in NATO, or conversely NATO's interest in Ukraine. It sees that Russia wants that buffer between it and the European region.

Can you comment a little on whether it could be both? Perhaps it's both. I don't want to put words in your mouth. I've always felt that it's his legacy, but through much testimony it's been said otherwise. Perhaps you want to comment on whether it's both or....

Col Viktor Siromakha: Yes, of course. I can provide you with some assessment.

In my personal opinion, Russia is like a mother-in-law. Once Russia sees that Ukraine is going to the European Union, to NATO, Russia becomes mad. Not only Russia, but Mr. Putin becomes mad.

For me, the brightest example of this madness was the Ukrainian success in 2012 when they had this incredible football championship in Ukraine in Kharkiv, Donetsk, Kiev, Dnipropetrovsk, and Lviv. Together with Poland, we organized and had an incredible football competition. Please, have a look at the stage there in Donetsk. Yellow and blue in Donetsk, no Russian colours. This is the central stadium of Donetsk. That's the brightest example of our success. We've been moving there. High-speed trains have been travelling from Kiev to Donetsk in four hours.

Then they saw what was going on and they decided they had to do something. They started this political assault of Ukraine, undermining our movement to the European Union.

● (1645)

Mr. Darren Fisher: I'll give my remaining time to Mr. Gerretsen.

The Chair: If you had any, I'm sure he'd appreciate it. Unfortunately, you don't.

Mr. Bezan.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Mr. Chair, I'll pass my time to Ms. Gallant.

The Chair: Ms. Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Thank you, Mr. Chair.

Over the years, there had been quite a resistance to acknowledging that cyber is a domain that they should be paying attention to, but even recently, they don't want to coordinate efforts among member countries. They say, “Well, politics has their own kind of system, and in other parts of Europe they've got their own. They're different people.” There are all these reasons we shouldn't be coordinating. They have a response centre where they'll help, central response.

Do you think that NATO should have a nexus or some centralized centre where they can share what's going on in terms of attacks, or is this done somehow already?

Mr. Alan W. Bell: One of the big issues from my perspective is.... I had a section called “Canada's Response to Hybrid Warfare”, and I was talking about the whole country. I asked why we didn't deal with this that way. I used the words “whole-of-government”. I think everyone I've listened to talk tonight is asking, “Whose responsibility is it, DND? Is it the government's responsibility? Is it somebody else's responsibility? Where is the money coming from?”

If we adopted a whole-of-government approach to this, maybe we would get somewhere, because at the moment everyone is thinking in silos, and that's not going to work with cyber. It works with lots of other things. Our approach to terrorism and putting organizations in silos that are supposed to communicate between each other, we know sometimes it's successful and other times it fails because people just don't talk.

It's the same with NATO. Every country in Europe is entitled to join NATO if the government of that country decides to do that. It's the same with the EU. The former Baltic countries are now saying they will have more success if they're in the EU financially, economically, and everything else. Also, if they're a member of NATO, they join a group of people, which as I said is now 29, and if something happens, and Russia tries to do something like this, there are 29 countries that are going to bite back. Unfortunately, we did not bite back. I'm not saying we invade them just because of what happened in the Ukraine or in Crimea, but we weren't strong enough to say, “Wind your neck in”. There are 29 countries, and most of them are on the Russian border.

Consequently, he is not being slapped on his wrist for what he's done. He'll do a little more, a little more, and a little more until one day NATO has to turn around and say, “Enough is enough”. When do we say that? When does NATO say that? Is it going to be this year, next year, the year after?

Russia is moving forward. They're getting better at cyber. They're getting better at all the other things. They have a huge standing army that is trained to fight in Europe, nowhere else, just in Europe. What is going to happen if we don't do something about it?

Mrs. Cheryl Gallant: Cyberwarfare in effect neutralizes article 5 because of lack of attribution. What they tell us is that they're not going to have a coordinated effort on this because our individual countries don't even have our own cyber-doctrine in place. We were told in the defence review that yes, we have a whole-of-government approach, but when asked about a Canadian cyber-command, like what the United States has, “We don't need it. Everybody we need is in Ottawa. They're just a phone call away or a short cab ride away."

Mr. Alan W. Bell: In 2016, NATO said they would regard that a cyber-attack against a member state will result in article 5 being activated. Crimea and Ukraine are not included in that. If he had attacked a country that was a member of NATO, would we have activated article 5? We don't know because he didn't do it, and he didn't do it because he's not stupid. That's where we stand.

If in a year's time he does attack one of the NATO countries, what's going to happen? I don't think we've even planned that far. I don't know what NATO is doing, obviously, because I'm just a normal individual, but he didn't attack a NATO country so article 5 was not activated.

● (1650)

Mrs. Cheryl Gallant: If there was a cyber-attack, for instance....

Actually there were some NATO parliamentarians meeting this May when Heathrow airport went down because of an IT outage and resurge. We all still wonder whether it was really that, or whether, for whatever reason, they didn't want to have fear up in the air and it was a cyber-attack but they weren't going to admit to it.

Mr. Alan W. Bell: If we look at the last 12 months of the Trump administration, they're still trying to figure it out and they have the resources and the budget to be able to go and look for who did this. They've come to the opinion that it was Russia that compromised the elections and they have proof of that. We haven't that proof in the Ukraine simply because we haven't had time, because there are not enough cyber-experts in there checking all the various different things that happened.

One of the things that Canada is not providing to the Ukraine is cyber-expertise. We're not participating in that, but we need to, because we need to find out what people who are participating found out about it so that we can learn from it for ourselves. By not being there, we're relying on them to tell us.

Mrs. Cheryl Gallant: You answered the question—

The Chair: I'm sorry. We're out of time for this particular question.

I'm going to give the floor to Mark Gerretsen.

Mr. Mark Gerretsen (Kingston and the Islands, Lib.): Thank you, Mr. Chair.

Mr. Bell, you talked earlier about Russia's involvement in the Donbass, the area they currently occupy. You said we don't know if Russia will go to the next level. What is the next level?

Mr. Alan W. Bell: The next level is pushing forward, going in with cyber, doing a cyber-attack for whatever reason, and then continuing to move forward, or to move to another country that isn't in NATO.

Mr. Mark Gerretsen: We heard from a witness in our last meeting, a former diplomat to Russia and the Ukraine, that in his opinion Russia's interest in occupying the area they're in is that they were—I'm paraphrasing here—almost invited into the area because the Ukrainians in that area were pro-Russia and wanted their presence there to be protected.

Would you agree with that?

Mr. Alan W. Bell: No, because I don't know. However, why did Russian special forces take all their uniforms off, and then when they put the flag up over Crimea, it was Crimean citizens who were seen to raise the flag of Russia?

Mr. Mark Gerretsen: Right.

Mr. Alan W. Bell: Was that contrived? Was it prepared in advance? We don't know who those people were.

Mr. Mark Gerretsen: Then you disagree with that notion.

Mr. Alan W. Bell: No, I don't disagree. I just don't know.

Mr. Mark Gerretsen: You just don't know. Okay, fair enough.

You said the response from the allies or NATO is negligible. Why do you say that?

Mr. Alan W. Bell: They haven't done anything about it. All they've done is just diplomatic means and all the other various—

Mr. Mark Gerretsen: What about the response of.... You're talking about, full on, being part of the conflict.

Mr. Alan W. Bell: No, definitely not.

Mr. Mark Gerretsen: Then to that degree, we have 200 soldiers there who are helping to train Ukrainian soldiers. Is that not partly a response?

Mr. Alan W. Bell: That is a response, but when they're up against someone such as Russia, which is a highly mechanized, highly trained team 200 guys to teach basic military tactics, medical, IED identification, and everything else is not really going to stop anything.

Mr. Mark Gerretsen: What is a response that you would deem not negligible?

Mr. Alan W. Bell: This could be happening, I don't know. I'm not privy to what governments are doing to governments. What is the Government of Canada and what is the Government of the U.S. talking to Russia about? How are they going through that?

There has been nothing visual, so the people in the Ukraine are seeing nothing done. There are countries sending in training teams: the U.S., the U.K., and Canada. We're all contributing a bit towards it.

Mr. Mark Gerretsen: The witness who I previously mentioned also said, we should be out of there—again, I'm paraphrasing—and let Ukraine sort out its own problems. I mean it's Ukrainian soldiers who are on the conflict line. Would you agree with that?

Mr. Alan W. Bell: No. We have more than one and a half million Ukrainians living in this country and having one and a half million Ukrainians means one and a half million votes.

● (1655)

Mr. Mark Gerretsen: Okay. This may have already been asked, but the company you're president of, Globe Risk International Inc., is it doing any work in the Donbass region right now?

Mr. Alan W. Bell: No.

Mr. Mark Gerretsen: Are you aware of any Canadian corporations or Canadian interests in that area?

Mr. Alan W. Bell: No.

Mr. Mark Gerretsen: You're not, okay.

Going back to the military assistance, do you have any specific recommendations for Canada in terms of what else we should be doing from a military perspective?

Mr. Alan W. Bell: We need to be doing more full-spectrum warfare training, not just basic training for soldiers.

Mr. Mark Gerretsen: What does full spectrum mean to you?

Mr. Alan W. Bell: It involves every single thing we have in our ability. I've already discussed that as I went over what is needed, and that includes special forces, diplomatic, legal, economic, and everything else. It's the final thing. We should do everything. We either do nothing or we do something that's going to make a difference. My belief from having worked in other countries, definitely not in Europe, is that unless you go in there and you start doing something that's being recognized by the country, people will believe that you're doing virtually nothing. It's just a token. You're doing a token effort to assist.

Mr. Mark Gerretsen: Do I have any...?

The Chair: You're on time to the second. Thank you for making my job easier.

The last formal question goes to Ms. Hardcastle for three minutes.

Ms. Cheryl Hardcastle: Thanks. I get last wraps, and I guess I'll pursue that same line then.

We've heard so much about how we have to expand our conceptualization of what a soldier is and what combat is. Then you talk about diplomacy, like real people talking to each other. I'm wondering what these person-to-person relationships would be like, because you said earlier in one of your testimonies that we need to deepen bilateral relations. Do you mean tangible, traditional things?

For instance, we talked about lifting the temporary visa requirement for visiting Ukrainians to Canada. Do you mean stuff like that, or are you talking about something more subtle that includes more that I don't see?

Mr. Alan W. Bell: The Canadian military involvement at this particular time is that we've trained 5,000 people and that is sufficient, but what have we trained 5,000 people to do? Is the training that we're giving them going to help them if Russia decides to roll over their border again somewhere else?

We need to look at.... That's what I'm saying, full spectrum. It's not just the military. It's government and everybody else being involved in it. There are a lot of things happening that we don't know about and we're not privy to, and that is the way it is. The Ukrainian government will have a checklist of what it would like to see from us, and if we don't provide the Ukrainians with what they think they require, they will go somewhere else, the U.S. or somewhere else. We have to sort of make a decision as a government on what we're going to do.

We've done a token, which is there now and working very hard and everything else, but there are lots of other considerations that we have to look at: political, economic, and all the other various different things. If we're going to protect the country from being annexed by a hostile force then we have to do a little bit more than throw 200 soldiers 18 miles away from the Polish border to train them in basics. That's all it really is, basics really. We're just going through the motions of basics.

The reason I believe we should do this is that I've been involved in Africa and in the Middle East where we've had to do this, and if we only go in there with half measures, I know what the consequences are. I've also been into Afghanistan on behalf of the Canadian government to do other work in Kandahar Province. I went in with all the promises and then halfway through, it became politically non-viable, so I was prevented from doing the other things we were going to do.

This was $65 million, one of the biggest deals that Canada put into Afghanistan before we pulled out, and while we were there, it worked. The whole thing worked, and we achieved the goals that we went in there for, but on the way down there was a lot of interference from various different areas about what we should do and what we shouldn't do. We went in there with a plan, but that plan changed depending on who was running that plan, and consequentially it was very difficult to work through armpits of bureaucracy. That's another problem, and we have to sort that out; otherwise, we just keep going round and round in circles

● (1700)

Ms. Cheryl Hardcastle: Is there still time?

The Chair: You'll get some more time, but this particular opportunity has dried up.

Ms. Cheryl Hardcastle: Okay.

The Chair: We have time left and very predictably I'll divide some time amongst everyone to make it fair. The Liberals, Conservatives, and NDP will get five minutes each.

Really quickly before we shift into that, the testimony that I've heard sitting here listening for a long time, and even during our visit to the Ukraine, there was a lot of gratitude for the support Canada had given. I certainly would describe that as a lot more than token. Can we do more? We're going to deliberate about what more we can do, and obviously provide recommendations to the Government of Canada, but my perception of what we were doing was very much appreciated and was making a difference. This is my perception of what I've heard from the Ukrainians throughout our journey on this discussion.

Having said that, Mr. Gerretsen, you have the floor.

Mr. Mark Gerretsen: Thank you very much. Going back to Mr. Bell, you were talking briefly recently about the low level, for a lack of a better expression, training. Is it your recommendation that we should also be doing some training and assisting with the higher levels within the military structure?

Mr. Alan W. Bell: If we're not training our own officers how to deal with hybrid warfare, it means the Ukrainians are probably not dealing with it either. Maybe what we have to do is to start at their high command and then work our way down through the ranks to—

Mr. Mark Gerretsen: I apologize, I'm really short on time. To that point, a lot of struggles are with the fact that the Ukrainian military still has the structure to it that comes from the former Soviet Union.

Mr. Alan W. Bell: Yes.

Mr. Mark Gerretsen: I think that one of the real struggles is how to reform that. The base that we went to, the base commander there had been the commander for 13 years. I have a base in my riding at which nobody is a base commander longer than two years. You are empire building after a while; it's just human nature.

How do you effectively deal with that problem?

Mr. Alan W. Bell: Time.

When you have a country that has been a Soviet bloc country for so many years, they're trained in their doctrine, they're trained in their military procedures and everything else, then all of a sudden the country decides it wants to go—

Mr. Mark Gerretsen: They haven't been part of the Soviet Union for—

Mr. Alan W. Bell: For 15 years.

Mr. Mark Gerretsen: Right. Look at other countries that gained their independence at the same time. Why haven't they had that same.... I don't want to get into why they haven't had the same struggle, but how much more time is required?

Mr. Alan W. Bell: If these former bloc countries are going to come into NATO and into the west full time, they're going to have to be retrained, re-equipped, to deal as a member of NATO, not as a member of an independent country or an independent member of a Baltic state. That's going to take time. All the countries involved are going to have to provide whatever they need.

I go back again to the Ukraine. The Ukraine comes to the Canadian government and says they would like this, and they explain why. We say yes, yes, or no, no, no. I mean it's the Ukrainian government that's asking for help, so we either help or we don't help.

Mr. Mark Gerretsen: Thank you.

Mr. Spengemann.

Mr. Sven Spengemann: Thanks very much for the time.

Mr. Bell, taking you back to the earlier conversation about a potential UN peacekeeping mission, do you see any signals at all that Putin is currently looking for a political off-ramp, or that he's interested in starting a conversation?

Mr. Alan W. Bell: I am not a political animal. I speak from experience. I don't want to speak from a political angle because what I am saying.... I know. I'm watching your faces, and your eyes, and you're saying “Oh, my God”.

I can only tell you what I think. I'm not saying for one minute that I am right, but I'm telling you what I think. I'm probably one of the very few people in Canada who has fought the Russians, because I was with the Mujahideen for nine months, fighting the Russians in the late eighties. I know what they're like. I know what they are like to fight. I know what they do.

They didn't have cyber in those days, but they had fear of reprisals, of Afghan women and children, because all the men had gone to join the Mujahideen, and I saw what the Russians did in those countries without cyber. So yes, you're getting it from me, from the experience of what I've done in my previous past when I was a younger guy.

Mr. Sven Spengemann: How would you characterize Canada from the perspective of Mr. Putin? Is it out of the question that we could take any other role than to remain partial in this conflict?

Mr. Alan W. Bell: We have a government. We have a Prime Minister. Diplomacy is obviously the best way to go. It depends on whether Putin, who has his own agenda, is going to listen to our Prime Minister, or the American president, or anybody else. At this moment he has his own agenda. He doesn't care and, unfortunately, we have a counterbalance called Mr. Trump in the White House.

● (1705)

Mr. Sven Spengemann: Colonel Siromakha, could I get your views briefly? How united is the European Union on the conflicts, in what needs to be done for Ukraine to potentially end this conflict?

Col Viktor Siromakha: Ukraine is waiting for an agreement to a political accord among the European Union countries because what is going on in Europe now is quite a sophisticated process. We are following news from Spain, from Italy. We heard what happened to Montenegro a few months ago and those are all countries of the European Union.

Mr. Sven Spengemann: Do you feel that Europe is unified on the question of Ukraine?

Col Viktor Siromakha: Europe has its own opinion, and we would like this opinion to be a little stronger.

Mr. Sven Spengemann: Thank you for that.

Thanks very much, Mr. Chair.

The Chair: Mr. Bezan.

Mr. James Bezan: Thank you, Mr. Chair.

I want to thank the witnesses for being here.

Colonel Siromakha, in addition to losing so many troops in this conflict I think that Canada and all NATO members owe a debt of gratitude to Ukraine because you're holding the line against one of the most powerful military machines in the world today. As Mr. Bell said, NATO was caught off guard and you helped buy NATO time to get ready and have the enhanced forward position.

Now is the time for us to do more for Ukraine, and I couldn't agree more with you. You mentioned a number of things on your list that you would like to see Canada provide. President Poroshenko also talked about RADARSAT images. Is that on the list as well, that you would like to see Canada reinstate the provision of that type of intelligence?

Col Viktor Siromakha: Yes. It could be very useful for our situational awareness because we really need this information to better understand what is going in the temporarily uncontrolled territory of Ukraine, over their temporarily uncontrolled border between Russia and Ukraine of approximately 400 kilometres, and up to the three official crossing points. Could you imagine how many unofficial points could be used by the Russians to deliver ammunition, fuel, Russian troops, whatever?

Once again, that's why satellite images could be very useful for our situational awareness.

Mr. James Bezan: In addition to Canadian, American, and U.K. troops training Ukrainian soldiers, when we were in Ukraine we heard from our guys at Yavoriv base that they are also learning from Ukrainian military members who have first-hand knowledge now of how Russia fights. Is there more opportunity for officer exchanges, as well as Ukrainians training Canadian and other NATO members on the hybrid war that Russia has been waging against the Ukraine?

Col Viktor Siromakha: Yes, definitely. It's an incredible opportunity to share this practical experience of how to fight in modern conditions. We are talking now about cyber, about hybrid war, but real, practical, modern combat is more visible, something more practical for soldiers to survive.

For instance, a great example of life hacks from Ukrainian soldiers is how you get water when you are blocked for days and weeks in an airport. Our soldiers found water in water heater systems in the winter and this water is better than what they've been drinking. This was incredible information for our Canadian partners who have been training our troops in the Yavoriv area. These basic military skills are very simple, but nevertheless these skills save lives.

Mr. James Bezan: Thank you. I have a couple of quick questions for other witnesses.

Mr. Chair, we should have Mr. Wright back, especially as we dive more into the NATO study, and possibly do that in camera with the proper security measures in place so that we can have a more in-depth discussion on what needs to be done. Now you're talking about cyber-defence and cyberwarfare and preventive measures. By preventive measures are you talking that we have an offensive side to our cyberwarfare?

Mr. Stuart Wright: Again, it's difficult to answer that question. That question's determined by the fact that we don't already have offensive capability. I can't speak to that. I can speak to the fact that current and previous governments have taken appropriate measures in those areas.

● (1710)

Mr. James Bezan: Thank you.

Mr. Bell, I appreciate your comments a great deal, especially as to NATO being caught off guard, that we haven't done enough. I know a lot is hypothetical, but going forward what else does NATO need to be doing to not only assist Ukraine but to prepare for the next muse by Vladimir Putin.

I know some people keep thinking that he's trying to reinvent the Soviet Union. I believe he's an imperialist; he sees himself as czar. He's a capitalist; he doesn't want to go back to the communist way. I wonder what you think NATO needs to do.

Mr. Alan W. Bell: We need to support Ukraine because that's where we have to make a stand. Not just Canada—

Mr. James Bezan: The entire NATO....

Mr. Alan W. Bell: —NATO, and everybody else. If we don't do that, I believe there will probably be another attack somewhere to try to do the same thing. We have to be consistent and say, if you do this again, we will respond. We're not going to go to war over this. I don't think that, and I wouldn't recommend it, obviously. At the end of the day, we have to show that we're going to support them with everything they need. That's why, when the Ukraine asks for this, this, and this, we should give it serious consideration. If we don't, as I said, and if somebody else doesn't do it either, it's basically leaving Ukraine out on its own.

If we allow Ukraine to fall totally, what's going to happen next? It's going to be a bigger problem. We have to make a stand now.

The Chair: Ms. Hardcastle, would you like another question?

Ms. Cheryl Hardcastle: Thanks.

Colonel, would you help us understand your vision, your view. You know our current funding arrangements for training are expiring. We want to understand the importance of the training to you and where you think we can be expanding or upping our game, based on some of the comments that you've heard from our other witnesses today. When you're done, maybe I'll ask Mr. Wright the same thing until my time expires.

Col Viktor Siromakha: Of course, the training that Canada is providing the Ukraine now, with Operation Unifier, is very important. In April 2017, during the visit of our defence minister Stepan Poltorak to Canada, during the negotiations we agreed to increase the level of training, for instance, from the tactic level which Operation Unifier is covering now, to the operator level, to a mid-level of our units.

Of course, I would like to underline Canada's role now in the Ukraine because Ms. Sinclair, who is a strategic adviser for the Ukrainian defence reform advisory board, is doing incredible work. She's personally responsible for the implementation of reforms on the united defence forces leadership. Those are exactly the things we've been talking about.

I'm 38 years old and I'm an officer of a new generation. Yes, we have incredible officers, generals, flag generals in Ukraine with real combat experience. Nevertheless, day by day, week by week, their generation is going. Let's hope that in future years, in five or 10 years, you'll see absolutely a new generation of Ukrainians who are highly qualified with great expertise including combat experience, proper language training. In this case, this approach will be very interesting for us. If Canada has an opportunity to provide the Ukraine with additional funding, it will be very interesting for training and for the professionalization of officers, and it will be an investment in the future of the Ukrainian armed forces. It means a condition of future peace in Ukraine as a state and in the region as a representative of eastern Europe.

Ms. Cheryl Hardcastle: Good.

Mr. Stuart Wright: I would concur with Viktor. In terms of the training, you have the next generation of cybersecurity specialists and experts who are coming out of academia right now. We need to put them in a position where they can train in real-world conditions, look at real operational playbooks. My recommendation, if you're asking, is to take a look at how successfully our counterparts in Israel have been with the IDF in maturing their troops. They're doing their necessary military service. They're getting trained by their SIGINT corps, and their cryptography and cyber-scrutiny specialists, and they're going in and working with industry once they graduate and hardening the skill set and commoditizing it globally.

I think we can follow a similar practice here in Canada, adopt that playbook and basically, take academia, and work very closely with industry, government, and also the Department of National Defence to basically align with those efforts. We need to not just churn them out, but start hardening them, give them the opportunity. We need to compare ourselves to the other threat actors in the world.

An APT1 Mandiant report several years ago indicated the Chinese had 130,000 cybersecurity specialists. I would estimate in North America and perhaps in the G7 at best, there are anywhere between 20,000 and 25,000 in the private sector alone, cumulatively. If you look at the Russians, in terms of cybersecurity, you see estimates are in the same ballpark range.

If you look at WikiLeaks and you take a look at what happened with the CIA, with disclosure, with Langley and their infrastructure, you see they have at least six or seven different divisions and the appropriate cyber-supporting structures. We need to look at the fact that we're being out-gunned, and we need to start engaging very early on, at academia, and start producing the next generation of cybersecurity specialists.

● (1715)

Ms. Cheryl Hardcastle: Thank you.

The Chair: We'll go for two minutes with Ms. Romanado, and then we'll close with somebody on the other side.

Ms. Romanado.

Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Thank you very much, Mr. Chair.

I'd like to thank you for being here today and for the excellent testimony that you provided us.

You were mentioning, Mr. Wright, about cyber. When I was in Israel for a visit, I met with the company that does the cybersecurity for Hydro-Québec, my home province. We have a company outside of Canada that's actually providing cybersecurity for our power grid in the province of Quebec, so I know we are very behind in terms of cyber-expertise.

We've heard today that we are being reactive in some regards, versus proactive. We've heard you mention the plan of action that we should adopt, for instance revise and adapt our DND doctrine, provide the handbook guidelines and the framework, and adopt the TTPs. We've heard a bit about the fact that it needs a whole-of-government approach to address this issue. We've heard that, from a macro-level, NATO has not rewarded the bad behaviour but hasn't really smacked them down in terms of invading Crimea.

These things are going to take time. We've also heard that we're experiencing on a daily basis in Ukraine that people are dying. We had four soldiers killed yesterday. My question to you, because we'll have to be doing these things in parallel, is what should Canada be doing in the short, mid, and long term to help resolve this?

We have Operation Unifier, but we need to be flying the plane at the same time as we're building it. Could you elaborate on what your suggestions are in the short and mid term?

Mr. Stuart Wright: Short term should be, first, a federated model, meaning inter-jurisdictional co-operation with our strategic partners, both here in North America and globally.

Second, start mobilizing the next generation of cybersecurity specialists and align yourselves with academia, industry, government, and military. We need to start training the next generation.

Third, provide funding and a mechanism by which we can communicate, either in an intelligence-sharing forum or at an advisory level, so that we're sharing actionable information at the appropriate time. Also, provide a mechanism so that we can share that without impacting the brands of companies or of the government, or causing brand impact awareness.

Mr. Alan W. Bell: Governments have to realize that Ukraine has now basically been attacked. What are we going to do about it? Until they come to solving that conundrum, we're not really going to know, because whatever the decision is, it's going to be a government decision.

The Ukrainians have a need at the moment, because the bad guys are knocking on their door. They want certain things. We should listen to them and try to give them what they need if it's within our power, because if we don't and Russia decides to move forward and be more aggressive, we can't turn around and say we wish we had done this because we just lost another country. If we don't stand firm now, we could end up having to fight a war in Europe as a result, because they're going to do it again and again and again before we do anything.

● (1720)

Mrs. Sherry Romanado: Thank you.

Col Viktor Siromakha: It's a little difficult to add something very practical to what my colleagues have said, but I would say that Ukraine has successfully survived the crash test from three years ago, in 2014. Since that time we have had more than 7,000 cyber-attacks, and now we more or less understand what is going on. Our cybersecurity structures are facing these and defending our critical elements of infrastructure in quite good ways.

Yesterday's attack showed us that, yes, we can do it now. It will be very interesting for our partners to come to Ukraine and get this practical experience from Ukraine to tell what is going on and exactly which attacks are coming. We could come to make a threat assessment analysis and create a well-protected environment for other countries.

Mr. Stuart Wright: Sherry, may I make one final comment? You asked about the short, medium, and long term.

We've seen absolute developments and I'm not going to get into details. In quantum computing, Canada needs to get into the game. We need to support the resources we have at academia and start putting dollars and measured resources to support those efforts. That is a game-changer for cyber.

Mrs. Sherry Romanado: Thank you.

The Chair: The last question goes to Mr. Bezan.

Mr. James Bezan: Thank you, Mr. Chair.

I want to go back to the discussion around a potential UN peacekeeping mission. We heard from witnesses here that Canada shouldn't be a part of it because we're so tied to Ukraine already and involved in their efforts, so we're not seen as the honest broker.

I want to get your feedback on whether you agree with that or think Canada, because of our reputation, could still go in there and lead a UN peacekeeping mission if the opportunity presented itself.

Mr. Alan W. Bell: No, I was the one who made that remark. Basically, what I meant by that was that Russia would probably object, in the UN, to Canada running that UN mission for the reason that we're very close to the U.S.

Mr. James Bezan: You're not the only one to say this to us, though. We've had other witnesses as well who have said that there's not a chance or a hope in hell.

Mr. Alan W. Bell: I think it would be a good opportunity for Canada to lead a UN mission because then it would show that we are putting up and not just ignoring things.

No, I think Canada should be a part of that mission. I think it's an integral mission. It's probably one of the most important missions that we can get involved in at the moment. There are a lot of other missions out there—and we all know which missions they are—and they lead nowhere.

Mr. James Bezan: Colonel, could you also provide your feedback on that?

Col Viktor Siromakha: Yes, of course. A future peacekeeping mission would be a turning point for the modern history of Europe. If Canada and NATO partners could all play a vital role in this future mission, it would save the situation because the worst-case scenario of the movement of Russia towards the west will jeopardize the situation in the whole region.

Except in eastern Europe, we have numerous regions in the whole world where we now observe confrontations of interest. It's better to stop it now than to fight the consequences of Russian intentions.

Mr. James Bezan: Mr. Bell, you've mentioned a few times that there are other examples that we should be using in how we deal with the war in Ukraine. What are you referring to? Are you referring to what coalition partners have done in Afghanistan or in Iraq, or do you have something else in mind where we build capacity as well as participate in a conflict?

Mr. Alan W. Bell: Afghanistan was a totally different war. They didn't have the capabilities of the Russians, but the Afghans threw the Russians out or made them withdraw, so they must have done something right.

What I'm saying is that instead of just giving them basic military training, we need to give them full-spectrum training. They need training right across the board. As I said, that involves everything, not just from a military perspective but also from a government perspective, an economic perspective, a financial perspective, a legal perspective, and all these other things.

If we decide on a whole-of-government approach to this, we should expect the same from Ukraine. We should expect it to do exactly the same thing. Then that way we're working on the same page, as opposed to working on what we think is right.

Mr. James Bezan: My final question is to the three of you. You appear in front of the committee and in the heat of discussion you think, “I wish I would have said that.” Is there anything that you want to leave as final comments, all three of you, before we adjourn?

● (1725)

Mr. Alan W. Bell: As for me, I got lucky because I didn't really know what to say and I didn't know where you were taking this as a committee. I looked at it as a big problem, and I thought, well, hybrid warfare has to go in there somewhere because that's the big threat. That's where I threw a lot of my time.

I also wasted my time on cyber because I'm not a cyber-guy and I didn't know we had a cyber-guy on here. If a panel has a specific agenda in mind, it would be great if the people who come or are invited to attend know what the agenda is so that they can answer what you want to hear, as opposed to just making it up.

Mr. James Bezan: Mr. Wright, do you have any final recommendations?

Mr. Stuart Wright: I'll leave the panel with one final comment. Canada needs to be in a constant state of vigilance. Cybersecurity needs to be woven into the fabric of everyday society.

Mr. James Bezan: Colonel.

Col Viktor Siromakha: I would add that Canada now plays a vital role and is completely involved and committed in relation to Ukraine. I would appreciate if next year, 2018, would be even more successful with the presidency of Canada in the G7.

The Chair: Canada wants, the Government of Canada wants, and this committee wants Ukraine to be successful. This committee will now have the opportunity and duty to put together some substantive recommendations to the government of what we can do better, what we can do more. That's our undertaking.

I want to thank you very much for your time and your appearance today in front of us. Thank you.

The meeting is adjourned.