HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Procedure and House Affairs

PROC • NUMBER 031 • 1st SESSION • 41st PARLIAMENT

EVIDENCE

Tuesday, April 3, 2012

Chair

Mr. Joe Preston

Standing Committee on Procedure and House Affairs

Tuesday, April 3, 2012

● (1105)

[*English*]

The Chair (Mr. Joe Preston (Elgin—Middlesex—London, CPC)): We will go ahead and start our meeting today. It's meeting number 31. We're here pursuant to an order of reference of Tuesday, March 6, the question of privilege relating to threats to the member from Provencher.

We have some guests today, and our meeting is broken into two parts. Let's go ahead and get started. I understand that you have some opening comments. Please introduce yourselves, and go ahead with your opening comments. We'll have questions from members right after.

Ms. Toni Moffa (Deputy Chief, IT Security, Communications Security Establishment Canada): Thank you, Mr. Chairman.

[*Translation*]

I am happy to be given the opportunity to appear before the committee today. My name is Toni Moffa and I am the assistant deputy minister or deputy chief of the information technology security program at Communications Security Establishment Canada, or CSEC. With me today is Scott Jones, the director general of our cyber defence branch.

I will begin with some opening remarks that summarize the mandate and activities of CSEC. The mission of CSEC, for over 65 years now, is to provide information and to protect information of importance to the Government of Canada.

[*English*]

As you may already know, CSEC leverages its leading-edge technology expertise and national and international partnerships to provide three key services to the government of Canada. First, we collect foreign signals intelligence in accordance with the federal government's intelligence priorities that are established annually by cabinet.

Second, we provide advice and services that help protect electronic information and information systems of importance to the government of Canada through our IT security program. This is the program that I am responsible for and representing today.

Third, while we are not a law enforcement, investigative, or regulatory agency, we do work with our federal partners in the security intelligence and law enforcement community in the form of technical and operational assistance that allows them, on their request, to leverage our unique expertise and capabilities at CSEC in the lawful pursuit of their own mandates.

All of our mandated activities are subject to numerous internal and external accountabilities and reviews, including the external and independent review by the Communications Security Establishment Commissioner, to ensure our strict adherence to applicable laws that govern our operations and to respect the privacy of Canadians.

I am the assistant deputy minister responsible for managing the IT security program. That program provides products and services that help prevent, detect, and defend against information technology security threats and vulnerabilities. In this capacity, we share a responsibility with other federal departments and agencies. We work with the Treasury Board of Canada Secretariat's chief information officer branch, with Public Works and Government Services Canada, and with the newly created Shared Services Canada to reduce vulnerabilities and diminish the success of IT security threats in federal IT systems.

For prevention purposes, we develop technical standards and guidance, which, when implemented by federal departments and agencies, help strengthen their IT systems' security and resilience. To detect and defend against IT security threats, we work closely with the Treasury Board of Canada Secretariat and Shared Services Canada, and with the additional cooperation of the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, and Public Safety Canada, we track the activities and methods of IT security threats seeking to steal or do harm to federal information systems, or to systems that the federal government cares about.

The contribution of CSEC to these shared efforts is to use our unique technical expertise, capabilities, and classified information to complement the commercial security technologies already available or in use by federal IT security practitioners. Commercial security technologies used in federal systems, similar to those used by individual citizens on home computers and networks, help track millions of publicly known threats, and prevent the success of cyber-activity that could result in the theft of sensitive, classified, or personal information, or an online criminal activity.

Similarly, CSEC has developed its own methods and operations to monitor federal government communication connections to the Internet, and to detect and defend against those IT security threats that are not in the public domain. For systems that fall victims to these activities, CSEC offers assistance for a focused and quick response to mitigate the IT security incident, and prevent it from recurring. Technical information on these IT security incidents that occur in one area or department is also shared across government IT departments, including the parliamentary precinct, in an effort to avoid similar IT security threat activities from occurring there.

In order to take greater steps to enhance IT security across the country, this information is also shared with our Public Safety Canada partners, who will share the information through their partnerships outside the federal government.

The Internet has evolved into an indispensable and useful tool for government operations, businesses and their financial transactions, social networking, and information sharing for citizens. However, with two billion users on the Internet, it is also an environment that is attractive to those who seek to take advantage of its inherent vulnerabilities for criminal or other nefarious activities. Through CSEC's IT security program, our products and services try to help prevent those things from happening on government networks, and we also help them recover when they become the victim of serious IT security threats.

That is my brief overview of CSEC and its IT security program. I'd be happy to respond to any of your questions.

The Chair: Thank you very much for your opening statement. It has brought more questions than answers to me, but I'm sure the members will help take care of that for me.

Mr. Albrecht, you're up first, for seven minutes, please.

Mr. Harold Albrecht (Kitchener—Conestoga, CPC): Thank you, Mr. Chair.

I want to thank our witnesses for being here today.

As I entered the room, I assured the witnesses that we were here today to learn a bit about what we can learn about this issue. Mr. Bard appeared before us earlier in our study. I think he gave us, as a committee, a pretty clear assurance that the actual security systems on the Hill are as secure as we can possibly ask for, and there's a lot of good activity going on surrounding the security.

Your entire address this morning dealt with IT security. As you know, we're dealing with another issue today that delves into some of that, but broadens out into the Anonymous group. Could you just tell me briefly what you're aware of in terms of Anonymous, how they operate, and what kinds of threats they may pose in terms of hacking into IT systems here on the Hill?

● (1110)

Ms. Toni Moffa: What we generally know about Anonymous is available from open sources mostly.

Certainly what we're interested in, when we look at groups or individuals such as these, are the techniques they use and some of the technical techniques they could use to conduct IT security breaches of systems for their own purposes and to meet their own ends.

Some of the techniques and methods that we try to mitigate against would address things like how to address a distributed denial of service attack or a spear-phishing attack, which is a luring attack on a system, and put measures in place that strengthen security overall on that system.

It would look at things that network owners could do at the perimeter of the network in terms of monitoring and looking for signs of alerts, responding to those quickly and mitigating the damage that they could cause, as well as looking internally to the systems to provide advice and guidance on how they can better protect themselves and their information holdings as well.

Those are the types of things we would look at in relation to those types of groups and individuals.

Mr. Harold Albrecht: Thank you.

The issue that we're looking at today, and through this study, deals with a threat as regards a parliamentarian to actually carry out their duties as a legislator to introduce legislation—a threat to do whatever they can to make sure that legislation doesn't pass. I think that's a pretty serious threat.

One of the challenges we face is how to determine who actually posted this threat in terms of accessing IP addresses and that sort of thing. Certainly we know that we have challenges here locally.

Is there any mechanism or are there any international arrangements that would allow us, if someone would post a threatening video on YouTube, to access the source of that and identify the person posing a threat that, I think, is a real threat to the entire democratic process?

Ms. Toni Moffa: The threat that you're referring to, I assume, is referring to—

Mr. Harold Albrecht: Mr. Toews.

Ms. Toni Moffa: —the posting of the videos.

From our perspective, it's not an IT security breach that we would deal with.

Mr. Harold Albrecht: No, exactly.

Ms. Toni Moffa: It would be best dealt with by an investigative body or agency that would do that type of investigation and leverage their partnerships.

Mr. Harold Albrecht: Do you have working relationships with other investigative bodies, whether it's FBI, Scotland Yard, or any other agencies that would allow our authorities to be able to investigate who in fact is behind a specific threat?

Ms. Toni Moffa: Our international partnerships are most closely aligned with those who conduct similar activities to our own, so those are not investigative bodies.

Mr. Harold Albrecht: Okay.

I want to go back to what you said at the first, that your primary responsibility is IT security. I respect that. I understand that. Do you have any advice for the committee in terms of how we can deal with this very amorphous Anonymous group?

I mean, we don't even who know they are. Obviously no one does. What advice would you have for a committee that's trying to prevent the kind of threats to the democratic process that I think this particular situation dealing with Mr. Toews and a piece of legislation that was proposed and actually threatening to short-circuit our work?

Ms. Toni Moffa: Unfortunately, the best advice I can provide only relates to IT security: how they may be breached and how we can prevent those.

As to other issues surrounding this situation, I'm not very qualified to respond to that.

Mr. Harold Albrecht: Thank you, and thank you, Mr. Chair.

The Chair: Mr. Toone, you have seven minutes.

● (1115)

Mr. Philip Toone (Gaspésie—Îles-de-la-Madeleine, NDP): Thank you, Mr. Chair, and thank you for your presentation. It's certainly enlightening.

I have to say the security establishment is probably the least known of all of our security services. I only learned about it in university, when one of your colleagues explained to me that he worked for you. I was very interested to hear what he had to say.

My understanding is that the security establishment's limitation is that your mandate is to seek security breaches that may happen outside the confines of Canada. You're kind of a firewall against threats that may come into this country. Is that an accurate reflection?

Ms. Toni Moffa: For the purposes of protecting federal systems, yes, we look at those connections to the Internet and activities going on there for any signals of threat activity that may cause harm to our federal networks.

Mr. Philip Toone: I certainly admit, you understand as well, that this is quite a task. The Internet is a network set up by the military many years ago, and specifically designed so that it could be entered into from just about any place, you could access it from just about any location. It was built so that there would be redundancies in case of failures or attacks in certain locations. It's a very difficult nut to crack. It's the beauty of the Internet. I think it's a highly democratic structure. I think the military has to be applauded for creating a democratic structure, but at the same time, any security agency is going to have a terrible time trying to detect threats and being able to deal with them appropriately.

Within the context of the threat we're looking at here, we were asked by Minister Toews—and just in passing, I'm sure we all wish him a speedy recovery. I understand he's still hospitalized, and that's never something I would wish on anyone. We're here because he was threatened specifically by a YouTube video that was posted, and my understanding is that in fact it was posted outside of Canada as well. So there was a YouTube video that was sitting on a server elsewhere. The very structure of the Internet makes it very hard to determine where it's residing. There are servers all over the place. Again, redundancies within the IP system would make it very difficult to determine where the fault lies and where the threat is coming from.

I'd just like to understand better. If your mandate is to protect us against foreign signals and intelligence, to protect the Canadian government and Canadians in general from IT security threats, threats that seek to steal or do harm to federal information systems, where does that fit in within our mandate here?

We started this with a YouTube video that was posted, so where is the threat exactly in the YouTube video? Is it possible that, if you click on the link for that YouTube video, a hack would automatically come into this country and possibly compromise your security here? Would that be a fair and accurate reason why we're worried about this particular YouTube video?

Ms. Toni Moffa: From our technical expertise perspective, a publicly available tool was used to post some information, in this case a video, to the Internet. So from information available to us, that is not an IT security breach in our minds, right? It's not a technical threat.

Mr. Philip Toone: Have you been called upon to investigate this? Has the security establishment actually been called to look into this particular so-called threat?

Ms. Toni Moffa: I'm aware there's an investigation ongoing, but it would be inappropriate for me to comment on that.

Mr. Philip Toone: If I understand your mandate, this wouldn't fall within your purview, would it?

Ms. Toni Moffa: Part of our mandate is to offer assistance to other federal departments, should they request it, in the pursuit of their own mandate. So there is an opportunity for them to use our technical expertise, upon request.

Mr. Philip Toone: Could you describe the threat, then? From your perspective, what is the threat?

Ms. Toni Moffa: In relation to this specific situation, or more generally?

Mr. Philip Toone: Within the mandate of the security establishment. Why would we call upon the security establishment?

Ms. Toni Moffa: I see, yes. What we look at are threats that are not publicly known. Commercial technologies do a really good job of taking care of publicly known malicious activity, occurring through malicious software. So your anti-virus software, your firewalls, have good methods and techniques in place to guard against that.

What we look at are threats they don't know about, derived from classified information, so that we can similarly complement commercial technologies to look for those types of activities and protect government systems from them.

● (1120)

Mr. Philip Toone: I have two minutes left. My understanding is that the YouTube video was posted as a reaction to what Mr. Toews said in the House regarding Bill C-30. He seemed to intone that a large number of Canadians were engaged in criminal activity because they used the Internet.

A lot of people reacted to that quite negatively. There was some fair comment that was done, and perhaps there were some comments that passed the line. I think in the particular case of this YouTube video, it passed the line.

I'm wondering, though, as a security threat to information systems, where is it? Where is the security threat?

Ms. Toni Moffa: From this video, from an IT security perspective, I don't see any.

Mr. Philip Toone: All right. Would there be another security service within this country that would be better placed to look at this? Who would have the mandate to cover this threat, and what threat is it exactly?

Ms. Toni Moffa: I would suggest it would be the investigative bodies at our disposal in government.

Mr. Philip Toone: It may not be an information technology threat so much as it would perhaps be a breach of the Criminal Code, for instance.

Ms. Toni Moffa: I'm sorry. I didn't hear the last part.

Mr. Philip Toone: Is it even an information technology threat?

Ms. Toni Moffa: In our opinion, no.

Mr. Philip Toone: We're perhaps looking more at a breach of civil or criminal codes.

Ms. Toni Moffa: I'm not an expert there, but yes.

Mr. Philip Toone: Okay. Thank you.

That's it for me, Mr. Chair.

The Chair: Thank you, Mr. Toone.

Mr. Easter, it's great to have you at committee today. You have seven minutes.

Hon. Wayne Easter (Malpeque, Lib.): Thank you. It's a pleasure to be here, Mr. Chair.

Thank you to the witnesses.

I take it from what you said that this incident is not what you would classify as a security breach.

Ms. Toni Moffa: An IT security breach....

Hon. Wayne Easter: You say it's more of a threat on an individual. As far as CSE goes then, you really don't have any role in the investigation. It would be more the RCMP or maybe foreign policing agencies. When you're dealing with the Internet, it's certainly not just a domestic issue.

Would that be correct?

Ms. Toni Moffa: I agree with that. Yes.

Hon. Wayne Easter: On the YouTube video and the Vikileaks—a number of incidents surrounding this minister—part of it relates to the lawful surveillance bill that is being proposed and I gather is now on the back burner.

From the public perspective—you may be able to help us out in this area—there is a lot of concern about Big Brother. Privacy is almost a thing of the past. There is a lot of concern about big government, Big Brother, so to speak, finding out a lot of information on individuals either through the Internet system or other means.

How do you see finding the balance in that regard? I know very well there is the need for the role you play in terms of security of our IT systems from afar, and there is the need within the country for security and privacy. On the other side of the coin, there are people's privacy concerns that they want to protect.

How do you find the balance in this new age?

Ms. Toni Moffa: In terms of the legislation in question, it has no effect on the authorities and mandate of CSE. Our own legislation certainly has measures in place to respect all applicable laws, including those that protect the privacy of Canadians. We certainly have a strict regime of policy and procedures internally that have been approved and reviewed by the Department of Justice. Our CSE commissioner reviews our activities annually and has always found them to be lawful.

Those are the checks and balances we have in place. We have an organizational culture that is very rigorous. Everyone is aware of their responsibilities and the measures they need to take. That is how we respond to that.

● (1125)

Hon. Wayne Easter: There is always the fear of people, though, that they're being spied upon. Certainly there's the incident with this minister and what seems to be a threat. But what I find, and I think probably many members around here would be of the same opinion, is that in the Internet age there's an article in the newspaper, and then in the comments section a lot of the comments that come in could almost be considered as hate mail.

I think that's becoming a serious problem. I don't know, Mr. Chair, how we're ever going to get around it, because people are allowed to send letters in to the comments sections on the Internet using false names. I think that if you have to sign your name to the article, you're less likely to make some of these outrageous comments that are being made against a person or in opposition to a policy issue.

I know this is not your area, but do you see problems in that regard? How do we start to get a handle on what I'm seeing increasingly as almost hate? It can develop on issues, but individuals are being attacked in the comments sections to the point that I hardly ever read them. It's an increasing problem.

Do you see that from where you sit?

Ms. Toni Moffa: Well, the Internet has evolved into a vast, complex infrastructure. There are two billion users today on the Internet, and the number is growing. There are hundreds of millions of websites and trillions of e-mails passed every day, so it's a very difficult environment to control—if it were even possible to control in that way.

Hon. Wayne Easter: I understand that, and there's no question that it's huge and evolving. But whereas at one point in time people had to sign their names.... I know they sign their names somewhere, and then they use this nickname.

The reason I raise this question is that in terms of this threat we're dealing with—Anonymous, whom we do not know even—each and every one of us who are not ministers but who take policy positions because it's part of our job, increasingly faces hate mail because the people who are writing the letters do not have to sign their names.

In your experience, are there any countries or any laws anywhere that try to get around that issue? I think it's escalating and that it leads to outrageous statements and outrageous attacks upon individuals. In this case it's an outrageous attack on the minister by Anonymous, but this isn't the only instance. I think all of us around here.... Somebody takes a dislike to something we said and then goes on a rampage. And in the comments section they go for the jugular, and it's nearly hate.

The Chair: I'll allow a quick answer.

Ms. Toni Moffa: I'm here as a technical expert. It's very inappropriate for me to provide any comments or suggestions in that regard.

The Chair: Thank you very much.

We'll go to a four-minute round.

Mr. Zimmer, you're starting us off.

Mr. Bob Zimmer (Prince George—Peace River, CPC): Thank you for coming today.

I asked this question at our last meeting. We ask for information and advice on how you can help us as parliamentarians, but I see this as an overall issue for Canadians in general. Canadians elected us, and we're their representatives; an attack on us is an attack on them. It can even happen in their daily lives that they're attacked or bullied or whatever you want to say.

I would ask you—you're the expert—how we would best protect ourselves from these IT threats in our jobs here and in our homes.

Ms. Toni Moffa: Some of the things that the CIO, Louis Bard, raised are good IT practices, many of which originate from our advice and guidance from an IT security point of view, and which would help prevent a lot of malicious activity from happening on networks or computers. Those are standards and guidance that could go a long way to making it very difficult for those seeking to do harm to do the harm that they do.

It also reduces vulnerabilities within our systems. There's no doubt that the Internet is a vulnerable place; there are many risks involved. As soon as you connect, there are risks associated with it. There are some steps to take to diminish those risks, but they will never go away entirely.

● (1130)

Mr. Bob Zimmer: Right.

I have another question. I'm sure you've dealt with the group Anonymous. I shouldn't assume that, but I want to ask you about your estimation of the membership of Anonymous. I think there are a bunch of different facets to it. There are the nefarious and there are the non-nefarious who want to be associated with the movement.

What would you say is the breakdown of serious criminal intent as part of the membership, as opposed to the number of association-seekers?

Ms. Toni Moffa: Unfortunately, I wouldn't be qualified to speak to their intent. What we look at is the techniques that are used by such groups and how to provide advice to prevent those things from being successful in our own systems.

So I would be unable to comment on that.

Mr. Bob Zimmer: Okay.

I have just one more, if I have time.

I want to know how your particular organization cooperates. How do we cooperate with other organizations overseas? How does that work, in terms of a relationship?

Ms. Toni Moffa: There are international partnerships with our direct counterparts, whereby we share information and technological capabilities with each other, because we have some common goals and objectives. Those would be our direct counterparts in the United States, the U.K., Australia, and New Zealand mostly—those whom we mostly deal with. More broadly, there are international groups in which we can cooperate, such as NATO.

Mr. Bob Zimmer: So we have an active relationship now.

Ms. Toni Moffa: There are venues for cooperation more broadly.

Mr. Bob Zimmer: Thank you.

The Chair: Thank you, Mr. Zimmer.

Madame Latendresse, you're up for four minutes, please.

[*Translation*]

Ms. Alexandrine Latendresse (Louis-Saint-Laurent, NDP): Thank you.

Thank you very much, Ms. Moffa, for your remarks.

Anonymous was just mentioned once again. Anonymous is not a closed group. Almost certainly, whoever posted the video on YouTube and threatened the minister probably has absolutely no connection to any hackers in the United States, Australia or anywhere else. People know that anyone can do these things using the name Anonymous, so I think it would be extremely difficult to say with any certainty that Anonymous is doing this, or that Anonymous has any such intentions. Anyone can use this label on their activities. I sometimes find it hard to determine where we are in all of this, because for now, as we heard earlier, we are talking about someone somewhere who posted a video online on YouTube.

Yes, some people who say they are from Anonymous did hack into the American federal systems, for example, but that is not what we are talking about right now.

When security breaches occur and hackers get into the American federal system, are you in contact with them to know what happened and how you can update your tools to prevent these kinds of threats? Do you have any contact with them in that regard?

Ms. Toni Moffa: Who do you mean, exactly?

Ms. Alexandrine Latendresse: I mean the American equivalent of your agency, for example.

Mrs. Toni Moffa: Yes, yes.

Ms. Alexandrine Latendresse: When security breaches occur in the U.S., you can discuss how to improve the system with them.

Mrs. Toni Moffa: We share our experiences, so we can help one another in order to prevent or deal with problems when they do occur in our systems.

● (1135)

Ms. Alexandrine Latendresse: Some problems occurred recently, a few months ago, I think, or not too long ago. Do you know if this has been done since? Has there been any dialogue in order to make the systems more effective and more secure?

Mrs. Toni Moffa: I cannot comment on that, and I certainly cannot comment on other people's experiences. That is considered classified information.

Ms. Alexandrine Latendresse: Coming back to Anonymous, if I understand correctly what you are saying, nothing has been done so far by anyone who reports to you.

Mrs. Toni Moffa: That is correct.

Ms. Alexandrine Latendresse: So you are here primarily to tell us about what you could do if something were to happen in the future, for example, if a hacker tried to—

Mrs. Toni Moffa: We are learning about the methods they use in an effort to prevent their actions in the future.

[*English*]

The Chair: Thank you.

Mr. Hawn.

Hon. Laurie Hawn (Edmonton Centre, CPC): Thank you, Mr. Chair, and thank you to our witnesses for coming.

Mr. Zimmer asked a question about good IT practices and so on. You said you do promote those. Are you able to share any specific good IT practices that might be useful for individuals?

Ms. Toni Moffa: There's plenty of advice and guidance that's available on our public website. That's openly shared.

In general it's about taking steps to put in place proper security measures at the perimeter, and that is monitoring for things that can happen so that we can react swiftly when they do happen. That helps to mitigate any damage that might be caused or limit the costs that would be incurred from a cleanup. Being vigilant is a very important one.

Also, there's looking at how we protect our information holdings within those networks. Certainly not all information is created equal, so some information deserves more protection than other information, and there are technologies that can be used for that.

User awareness is a big one—user awareness and education, not only for IT security professionals and practitioners, but also for regular users of the Internet, of computer systems, to warn them of the risks and dangers and how they may be vulnerable. For instance, managing their passwords is a good one, changing them often, what's a good password, things like that.

There are a lot of things. One of the key pieces is that the software that we use on our networks is constantly being updated and upgraded with security patches. Once vulnerabilities are discovered, vendors are very good at putting out patches to upgrade their products so that they can avoid those vulnerabilities from being exploited. Swiftly patching systems and networks, and the applications on them, is a very good way of preventing threats and risks associated with them.

Hon. Laurie Hawn: That's not something the average home user would be able to do, though.

Ms. Toni Moffa: The average user would find that all bundled into their anti-virus software or their security software on their computer.

Hon. Laurie Hawn: Everything we've heard suggests that our chances of catching Anonymous, whoever he or she or they may be, is pretty remote. I guess it varies, but do you see these guys or gals as pros, or enthusiastic amateurs?

Ms. Toni Moffa: Certainly it doesn't take much technical expertise to post a video.

Hon. Laurie Hawn: So probably they're enthusiastic amateurs.

You mentioned in your remarks about detecting and defending against those IT threats that are not in the public domain. Without getting too detailed, in regard to the extent of the IT security threat, public domain or non-public domain, is it safe to say that's increasing? Is it something we think we can keep ahead of? How tough a challenge is that?

Ms. Toni Moffa: No, I wouldn't say we're keeping ahead of it. We're trying to track as many as we can, and those numbers increase exponentially. It's very difficult to keep pace with the number of threats we see out there.

Hon. Laurie Hawn: Okay, I'll leave it at that.

For the Luddites among us—and I refer to myself—could you describe spear-phishing?

Ms. Toni Moffa: Spear-phishing is a technique. One of the ways someone can take advantage of your computer, your network, and the information that it contains is to send you an e-mail that looks like a legitimate e-mail, which would have an attachment that would look very attractive to you or be of interest to you. By clicking on this attachment you would get a document pulled up. To the user there's no apparent change, but in the background there would be some things happening to install something on your computer that could be used later to steal or extract information from your computer network.

Hon. Laurie Hawn: Not to be too paranoid, but we've had this discussion before, about all the little data sticks that you get from everywhere. If you turn them over and see where they're made, would that cause you any concern about not knowing what's actually on that stick?

● (1140)

Ms. Toni Moffa: That's right. We increase our vulnerabilities as we increase the things we attach to our networks. So thumb drives and mobile devices increase the ways into our network and make them more vulnerable.

Hon. Laurie Hawn: So it would be pretty easy for somebody—for a pro, not an enthusiastic amateur—to embed something on a data stick that you receive as a gift, and you stick it into your computer and who knows what happens.

Ms. Toni Moffa: It's possible.

Hon. Laurie Hawn: Thank you.

The Chair: I have no one on the question list. If that's it for these witnesses, we'll suspend for a moment.

I thank our witnesses for coming.

Let's bring forward our second panel for today.

We will suspend for a minute or two while we do that.

Thank you very much for your help today. It was great to have you.

● (1140)

(Pause)

● (1140)

The Chair: We'll go ahead and start the second part of our meeting.

We have with us today Robert Gordon from the Canadian Cyber Incident Response Centre; James Malizia from the Protective Policing Branch; and Tony Pickett from the Technological Crime Branch.

Mr. Gordon, do you have an opening statement? Okay.

If we have an opening statement from our RCMP friends, we'll go ahead with that and then we'll do questioning.

Go ahead. Please start.

Mr. Robert Gordon (Special Advisor, Cyber Security, Canadian Cyber Incident Response Centre, Department of Public Safety and Emergency Preparedness): Thank you, Mr. Chairman, and honourable members of the committee. Thank you for giving me the opportunity to speak to you today.

I have one minor correction for the record. I'm actually with the Emergency Management and National Security Branch, the Cyber Security Directorate, in Public Safety. I've taken note of the committee's proceedings today and thought it might be helpful if I begin my remarks with a brief overview of the government's approach to cyber-security. I'll then elaborate on the role of the Cyber Incident Response Centre, which is part of the National Cyber Security Directorate located in Public Safety Canada.

Let me start by drawing your attention to Canada's cyber-security strategy, which was launched in October 2010 by the Minister of Public Safety, the Honourable Vic Toews. The strategy signals the government's commitment to strengthening the security and resilience of Canada's vital systems and our approach to doing so. That approach is founded on the idea that securing cyberspace is a shared responsibility, one in which we all have a role to play. In implementing the strategy, Public Safety Canada is therefore striving to ensure clarity of roles and responsibilities within the Government of Canada and to establish the partnerships we need with other levels of government, the private sector, academia, and international allies.

Permit me to offer a high-level snapshot of those departments and agencies with an operational role in cyber-security so as to situate the roles of Public Safety Canada and the Canadian Cyber Incident Response Centre in context. In support of Public Safety Canada's mission to build a safe and resilient Canada, the National Cyber Security Directorate leads and coordinates the development and delivery of policies and programs that increase the resiliency and security of the vital systems and their information that underpin Canada's national security, public safety, and economic prosperity. Within the National Cyber Security Directorate, the Canadian Cyber Incident Response Centre is responsible for helping to mitigate, respond, and recover from incidents affecting vital systems outside of the federal government. Since these systems are owned and operated by other levels of government and the private sector, partnerships are essential to strengthen their security. The Cyber Incident Response Centre also works closely with federal intelligence and law enforcement agencies as well as international allies in delivering on its mandate. In the event of a national level cyber-incident, the Cyber Incident Response Centre would play a key role in the coordination of that event.

The Communications Security Establishment, who just appeared before you, along with organizations such as Shared Services Canada, and independent departments and agencies, including Parliament, all have roles in the prevention and the management of cyber-incidents on federal government systems. Two other agencies, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, have investigative roles that encompass systems both inside and outside the federal government. CSIS investigates cyber-activities that raise national security concerns or appear linked to threats to the security of Canada. The objective of their investigations is to assess threats, and produce intelligence for the government. Law enforcement agencies, whether the RCMP, provincial, or local forces, investigate cyber-incidents that are suspected of being criminal in nature, be their origins domestic or international. The RCMP also conducts national security criminal investigations, as CSIS does not have a law enforcement mandate. The purpose of law enforcement investigations is to prosecute criminals in court.

Clarity of these roles and responsibilities is vital not just for efficiency and effectiveness, but also for focused and rapid response to incidents. For instance, when investigations are initiated evidence must be preserved even as we work to mitigate and recover systems. Since attacks detected on one system will often affect others, the rapid sharing of information between, for example, the Communications Security Establishment, which is acting to protect the government, and CCIRC, which is trying to share its information with its partners, is essential.

Let me turn now to setting out in greater detail how the Cyber Incident Response Centre delivers on its mandate to contribute to the security and resilience of the vital cyber-systems that underpin Canada's national security, public safety, and economic prosperity. As Canada's national computer emergency readiness team, CCIRC's role is twofold: it monitors and provides mitigation advice on cyber-threats, and it coordinates the national response to major cyber-security incidents. As such, the Cyber Incident Response Centre is Canada's national coordination centre for the prevention, mitigation, and response to cyber-events.

● (1145)

To fulfill its role, the Cyber Incident Response Centre provides authoritative advice to, and coordinates information sharing and event response among all levels of government, international counterparts, critical infrastructure operators, the private sector, and information technology vendors. These activities are focused on providing assistance and coordination to resolve the incident and to bring operations back to normal.

CCIRC is not an investigative body. It does not have law enforcement or regulatory authorities. The Cyber Incident Response Centre works under the premise that prevention and preparation are the most effective ways to enhance Canada's cyber-security. We act as a trusted broker for information on threats, vulnerabilities, and mitigation techniques. We have our own technical capability, and we invest considerable effort in forging trusted relationships that lead to an exchange of detailed, actionable information. Since these relationships often involve the disclosure of information that our partners consider to be either proprietary or potentially damaging to their public reputations, we guard their privacy fiercely.

CCIRC aggregates and analyzes the information it receives in confidence from sources both inside and outside the government. We then develop mitigation advice and best practices for our partners to use in defending their cyber-infrastructure, while protecting sources. Through our various information and guidance products, as well as through briefings in trusted settings, Public Safety Canada also raises awareness of the need to take greater steps toward cyber-security.

In short, during an incident, CCIRC collaborates with the affected organization to help bring it back up and running, ensures that our federal partners are apprised of how they can use the information to fulfill their mandates, and develops mitigation advice so that other organizations and sectors can take appropriate precautions.

Cyber-incidents and attacks occur frequently, but vary greatly in severity. In many cases, they are merely a nuisance, and the cyber-community is capable of defending itself against them. Nonetheless, some cyber-threats have the potential to escalate into something more serious. For this reason, the Cyber Incident Response Centre dedicates time and resources to maintain awareness of potential cyber-threats and their potential impact. The early identification of a cyber-threat allows us to better understand it, and therefore better contain it, should the threat escalate.

Ultimately, the federal government and agencies involved in cyber-security remain committed to the protection of Canadian networks. While we all have our roles to play, collectively we share the premise that our cyber-security is indivisible. If the government is being hit, in all probability so are others, and vice versa. We will continue to collaborate with domestic and international partners to identify and mitigate threats as they arise in order to enhance the safety of Canada's digital infrastructure.

Thank you for your attention, and now on to your questions.

● (1150)

The Chair: Thank you very much.

Assistant Commissioner Malizia.

Assistant Commissioner James Malizia (Assistant Commissioner Protective Policing, Protective Policing Branch, Royal Canadian Mounted Police): Thank you, Mr. Chair.

The Chair: You have a short statement. Please, go ahead.

A/Commr James Malizia: Yes, thank you, and my thanks to this committee for providing the RCMP with an opportunity to appear today.

With me is Superintendent Tony Pickett, the officer in charge of the RCMP's Technological Crime Branch.

[*Translation*]

I would like to begin by addressing the issue of threats to the member for Provencher.

Ministers of the crown are entitled to receive RCMP protection in Canada and abroad, as needed, by virtue of section 17 of the Royal Canadian Mounted Police Regulations. If a minister or a member of Parliament feels their safety and security is in jeopardy, they should report it to the RCMP or the local police of jurisdiction.

Based on an evaluation of the information provided, the RCMP will assess the need for protective services and, if warranted, may initiate an investigation. We constantly review and monitor the security measures put in place for our protectees, and if needed, we will adjust our security package accordingly. Security packages are provided on a case-by-case basis, are intelligence led, and are commensurate with threat and risk assessments.

[*English*]

I'd like to begin by addressing the issue of threats to the member for Provencher.

Ministers of the crown are entitled to receive RCMP protection in Canada and abroad, as needed, by virtue of section 17 of the RCMP regulations. If a minister or a member of Parliament feels their safety and security is in jeopardy, they should report it to the RCMP or the local police of jurisdiction. Based on an evaluation of the information provided, the RCMP will assess the need for protective services and if warranted, may initiate an investigation.

We constantly review and monitor the security measures put in place for our protectees, and if needed we will adjust our security package accordingly. Security packages are provided on a case-by-case basis, are intelligence led, and are commensurate with threat and risk assessments.

We take all threats to ministers and members of Parliament very seriously, whether the threats are in the form of a threatening letter, in person, or through electronic or social media.

The Internet has revolutionized the way we communicate and has transformed our society. It continues to influence society at a pace and rate of growth that is on an exponential trajectory. These new and evolving technologies have brought about much positive advancement: instantaneous communications worldwide, the ability to share knowledge and to work collaboratively to more effectively conduct commerce, and the list goes on.

Nevertheless, these profound advances have their dark side and that is the use of technology for the purpose of cybercrime. The RCMP views cybercrime as any crime committed using a computer network and/or hardware device. The computer network or device could be the agent of the crime, the facilitator, or the target of the crime.

Advances in technology have created an environment where individuals achieve anonymity. Criminals exploit the faceless environment provided by the Internet to conceal their identity and conduct serious criminal activity.

● (1155)

[*Translation*]

Criminals are reinventing themselves online to facilitate criminal acts associated with fraud, facilitation of drug trafficking, sexual exploitation of children and money laundering, for example. At the same time, new cybercrimes have emerged, including hacking and theft of data where the computer, the network or data become the focus of the criminal activity.

As you know, the Internet and various forms of social media are being used as a means to promote social change, and for individuals and groups to express their freedom of expression. This can be positive when done in a lawful manner. Such campaigns can be compared to online versions of protests on Parliament Hill, petitions and peaceful protests.

[*English*]

Criminals are reinventing themselves online to facilitate criminal acts associated with fraud, facilitation of drug trafficking, sexual exploitation of children, and money laundering, for example. At the same time, new cybercrimes have emerged, including hacking and theft of data where the computer, the network, or data become the focus of the criminal activity.

As you know, the Internet and various forms of social media are being used as a means to promote social change, and for individuals and groups to express their freedom of expression. This can be positive when done in a lawful manner. Such campaigns can be compared to online versions of protests on Parliament Hill, petitions, and organizing peaceful protests.

The vast majority of those who use social media to reach out do so with positive intentions and within the law, however, there are others with very different objectives and methods of achieving their goals. Certain groups would have us believe that they are the sole agents of social change. Our current understanding of some of these cyber-groups is that they can be best described as a movement with undefined membership. They offer a forum for like-minded individuals or groups to express similar ideologies. Few of these individuals or groups represent themselves as criminal organizations. However, their tactics sometimes violate criminal laws in countries where they purport to operate.

[*Translation*]

Cybercrime is growing at an alarming rate around the globe. Investigating cyber-threats or cybercrime is an evolving and challenging domain. However, the RCMP remains committed to enforcing the laws, apprehending criminals and providing for a safe and secure Canada.

[*English*]

Cybercrime is growing at an alarming rate around the globe. Investigating cyber-threats or cybercrime is an evolving and challenging domain, however the RCMP remains committed to enforcing the laws, apprehending criminals, and providing for a safe and secure Canada.

Thank you.

The Chair: Thank you very much. Thank you both for your opening statements.

We'll go to questions by members.

Mr. Albrecht, you may start. You have seven minutes.

Mr. Harold Albrecht: Thank you, Mr. Chair. Thank you to all of you for being here today.

One of the most encouraging things about our investigation to this point, for me at least, has been the incredible commitment to sharing. Mr. Gordon, you indicated that very clearly at a number of points throughout your opening statement—the fact that the different groups that are responsible for various aspects of security have a good network of communication.

In the RCMP statement, Mr. Malizia, you pointed out that you take all threats to ministers and members of Parliament very seriously, whether the threats are in the form of a threatening letter, in person, or through electronic or social media.

I wanted to read into the record some of the threats that were posted on YouTube by this group that identifies itself as Anonymous.

> We demand that you scrap the bill in its entirety and step down as safety minister. We know all about you Mr. Toews, and during Operation White North we will release what we have unless you scrap this bill.

They go on to say, "Anonymous demands the immediate resignation of Vic Toews, the scrapping of Bills C-30 and C-11 in their entirety...".

It's clear to me that there's no physical threat to Mr. Toews, at least not in this particular statement. But to me, there appears to be a definite threat to democracy, and I've mentioned this earlier, in the sense that legislators are sent here to craft legislation to improve the safety and security of our citizens. So it seems to me that this threat is a very real threat that all members of Parliament, and especially, members of the crown, the ministers, need to take seriously.

In your opening statement on page 5, Mr. Gordon, you indicated that CCIRC is not an investigative body and it does not have law enforcement or regulatory authorities. Prior to that you said:

> Law enforcement agencies, whether the RCMP, provincial, or local forces, investigate cyber-incidents that are suspected of being criminal in nature, be their origins domestic or international. The RCMP also conducts national security criminal investigations, as CSIS does not have a law enforcement mandate. The purpose of law enforcement investigations is to prosecute criminals in court.

Going back to my line of thinking that this is a real threat to democracy, it's a threat in the sense that parliamentarians are intimidated from doing their work and then, perhaps, we could even argue that it may be a threatening factor in terms of those who are considering public service. So where in the continuum of criminality do you see this current posting of a video by the group that identifies itself as Anonymous? Is a criminal investigation necessary? What kind of investigation would be called for in terms of trying to identify who the people are who are responsible for posting a threat of this nature?

Whoever wants to may respond to that.

● (1200)

A/Commr James Malizia: Thank you, Mr. Chair.

Although I'm not in a position to speak about any ongoing investigations, our current understanding of some of these cyber-groups is that they can best be described as a movement using a common banner with undefined membership. They offer a forum for like-minded individuals or groups to express similar ideologies. Few of these individuals or groups represent themselves as criminal organizations, however, their tactics sometimes violate criminal laws in countries where they purport to operate.

Historically, some threats to a minister or an MP that we have investigated have resulted in criminal charges. All I can say is that the RCMP would pursue a criminal investigation upon receipt of that information.

Mr. Harold Albrecht: Okay.

In terms of the sharing of information across jurisdictional lines, you mentioned sharing information internationally as well. What tools are at your disposal to pursue that in terms of identifying the IP address, or if we need to find the origin of something like this posting on YouTube?

A/Commr James Malizia: We work with law enforcement partners from around the world. With respect to cybercrime, we use the Interpol network, the RCMP liaison officer network, the G-8 24-7 network, which has approximately 60 member states, as well as sharing information on a police-to-police basis. We have information-sharing agreements with those countries. As stated earlier, international cooperation and the exchange of best practices is what enables us to work together and have positive results.

Mr. Harold Albrecht: This is my final question. We're struggling as a committee to try to identify exactly how we deal with this. This is the first time we've dealt with something like this. We've dealt with anonymous letters in the past, and I think we indicated that earlier. But an anonymous letter is slightly different from a posting a YouTube video that can be viewed by thousands or millions of people.

What advice would you have for our committee in terms of trying to mitigate the kinds of threats that may be posted, especially those targeting public officials whose job it is to increase the safety of all of our citizens?

A/Commr James Malizia: I would defer to my colleague here from Public Safety. As you know, the RCMP is not mandated to do cyber-security.

Mr. Robert Gordon: I think, as was said by one of the previous speakers, the actual posting of the YouTube video wasn't a cyber-event in the traditional sense, so Public Safety Canada doesn't provide advice on it. We have provided advice on protecting the various networks, but the actual posting of a video is a fairly easy thing to do. Unfortunately we're not in a position to provide much advice on that.

● (1205)

Mr. Harold Albrecht: Again I'm showing my lack of technical expertise as it relates to the Internet, certainly.

So there's no way, there's no technical way, of finding the IP address of the person who uploaded that threatening video, which would actually threaten the job of a member of Parliament or a minister of the crown?

A/Commr James Malizia: What I can say, Mr. Chair, is that each investigation is unique. In some instances we may be in a position to identify the individuals involved in criminal activity, and depending upon the complexity, we may not.

Mr. Harold Albrecht: Thank you.

The Chair: Thank you.

Mr. Comartin, you have seven minutes.

Mr. Joe Comartin (Windsor—Tecumseh, NDP): Assistant Commissioner, just so we're clear, and maybe more for people who are listening than for us, you're not capable, if I understand, of telling us whether or not the RCMP is conducting an investigation into this matter?

A/Commr James Malizia: My understanding is that it has been made public that there is an ongoing investigation.

Mr. Joe Comartin: That was going to be my next question.

When the minister was before us, he indicated that he had requested that the RCMP conduct an investigation. Can you confirm that?

A/Commr James Malizia: Yes, we have received information.

Mr. Joe Comartin: Can you confirm that the investigation's ongoing?

A/Commr James Malizia: I can say that there's an ongoing investigation.

Mr. Joe Comartin: Thank you.

With regard to the—and again I recognize the difficulty you have in terms of any details—attempt to identify who posted that YouTube video on the Internet, are there agencies other than the RCMP involved in trying to trace that?

A/Commr James Malizia: I'm not in a position to discuss any details or specifics with respect to any ongoing investigation.

Mr. Joe Comartin: All right.

Assuming there isn't an ongoing investigation, in terms of the ability to track a site like that, would that expertise lie within the RCMP offices or with CSE or some other agency, Mr. Gordon?

Where is the greatest expertise in our system to track?

Mr. Robert Gordon: I'm not sure I completely understand the question.

Mr. Joe Comartin: Let me repeat it.

Who is best able to identify who put that YouTube video up on the Internet?

Mr. Robert Gordon: I don't know the answer to that question, but perhaps Mr. Pickett would.

Superintendent Tony Pickett (Officer In Charge, Technological Crime Branch, Royal Canadian Mounted Police): I could probably speak to that question. There are groups of specialists in different government departments that collaborate quite often on these types of cases.

The complexity of the cases usually indicates that there's not one sole pocket, so we often share resources within the government departments and/or sometimes with other international agencies, law enforcement agencies, or intelligence agencies.

So I guess the expertise doesn't lie necessarily in one particular spot. We'd have to look at it on a case-by-case basis and reach out to other government departments and/or other federal agencies to help us with these kinds of cases.

Mr. Joe Comartin: Would that extend to reaching out to other countries?

Supt Tony Pickett: Absolutely.

Mr. Joe Comartin: We know that there have been charges laid in England and in the United States against people claiming to be part of Anonymous. Would that type of reaching out include reaching out to actual cases in other countries, and asking to share information with those other countries?

A/Commr James Malizia: Although I can't comment on investigations that have been conducted in other countries, we regularly exchange and share with various other agencies from around the world, whether they be best practices or collaborations on investigations.

● (1210)

Mr. Joe Comartin: All right.

Assistant Commissioner, with regard to the actual charges, are you able to answer any questions with regard to the types charges? And, I'm sorry, this came up in the last meeting around the difficulty with double-jeopardy—us making recommendations, for lack of a better term, on punitive action through the House of Commons versus criminal charges through the criminal justice system. That's your side of the coin.

Has any analysis been made of the types of charges that could be laid in these circumstances?

A/Commr James Malizia: Well, there are different charges, as you know, that are available to us through the Criminal Code. It could range from unauthorized use of a computer, under section 342; the use of, possession of, or trafficking of computer passwords; mischief to data; extortion; intimidation; and uttering threats. So there are different ones available to us through the Criminal Code.

Mr. Joe Comartin: We're trying to get some sense of timelines here, but I know you're not going to be able to answer that, so I won't ask the question.

In terms of the ongoing investigation, does it include physical threats? Or is it simply YouTube?

A/Commr James Malizia: I'm not in a position to provide you with any information at all.

The Chair: I thought that was going to be the answer.

Mr. Joe Comartin: I knew that was going to be the answer, Mr. Chair.

The Chair: You have a minute left if you want to—

Mr. Joe Comartin: I have no other questions. It's not going anywhere.

The Chair: Mr. Easter, for seven minutes.

Hon. Wayne Easter: Thank you, Mr. Chairman, and thank you to the witnesses.

Mr. Albrecht, in his questioning, read some of the threats from YouTube. He basically implied in that question that asking for a minister's resignation should be seen as a threat. I would hope not. I think I've asked for some and I don't want to walk out of here in handcuffs.

I don't see asking for a minister's resignation as a threat, not in any way. I think we've asked for a few.

Also, in your statement, you said that the minister has asked for an investigation. In your remarks to us, Assistant Commissioner, you said, and I quote:

> If a minister or a member of Parliament feels their safety and security is in jeopardy, they should report it to the RCMP or the local police of jurisdiction.

Did Minister Toews ask for such police protection?

A/Commr James Malizia: We have, in the past, provided protective services to ministers who have received threats, depending upon the threats. The security packages provided have been varied. We continue to assess, of course, through threat risk assessment, those threats that are reported to us, and at that time we do make a determination whether protective services would be provided.

As you know, I'm not at liberty to discuss what protective services we are providing or not.

Hon. Wayne Easter: So we can't determine whether or not Minister Toews has made the request.

I'm well aware of protection for ministers in the past.

So you can't tell us. We know Minister Toews has made the statement to the House and that's why this committee is discussing the issue, but you can't tell us whether or not Minister Toews requested security as a result of this.

A/Commr James Malizia: What I can tell you is that it is the RCMP that makes the determination of whether security is provided or not through a threat risk assessment.

Hon. Wayne Easter: Okay. Thank you.

It seems to me that in the evidence presented previously, and by both your groups, the various agencies are set up to deal more with threats to the system. Certainly the RCMP is set up to deal with threats to individuals, and that's your judgment call.

But is it fair to say that all the various security apparatus and various agencies we have in terms of this Internet age are set up more so to deal with threats to the system as a whole rather than to individuals? We are dealing with different circumstances in the way that this threat came forward.

Mr. Gordon.

● (1215)

Mr. Robert Gordon: Mr. Chairman, that's probably a good way to broadly characterize the responsibilities. We're looking at the integrity of both the data and the systems. We're looking at the confidentiality of data, ensuring that whatever is on the systems remains confidential. We're looking at the integrity of the data, so someone isn't going in and changing what the data is; and also at the availability of the data, that you're not denied access to your information in a variety of ways. So that's a good characterization of it.

Hon. Wayne Easter: In your remarks, Mr. Gordon, on page 2 in the English copy you said that the CCIRC is responsible for helping to mitigate, respond, and recover from incidents affecting vital systems outside the federal government, and you emphasized the word "outside". What about inside the federal government? What happens there? Why did you emphasize the word "outside"?

Mr. Robert Gordon: It was primarily to differentiate between the roles and responsibilities of the Communications Security Establishment, which provides the technical expertise and guidance for the Government of Canada's systems, and the responsibilities within Public Safety, which focus outside the federal government to provide the knowledge and best practices that the federal government has to a range of outside customers and clients, from provincial and territorial governments to some of the critical infrastructure sectors.

Hon. Wayne Easter: And you also talked about your response to cyber-events. I'm going to run out of time, so I'll ask two questions at the same time, Mr. Chair.

In layman's terms, can you give us the process of how you respond to those cyber-events in terms of attacks on the system, trying to mine data, trying to misrepresent, misinformation, or whatever?

My second question is really to the RCMP. If, in this case, Anonymous is identified and is found to be just south of the border or outside the country somewhere, what's the process? How do you, then, get at the individual in terms of charging them with a crime and getting them to face the consequences of that crime in this country, when it happens over the Internet, outside the country?

So there are two questions, one to Mr. Gordon and one to the assistant commissioner.

Mr. Robert Gordon: We produce a variety of information products for all of the people we deal with outside the federal government, ranging from very technical responses to more broad, information-based notes, and information or advisories on vulnerabilities that we're seeing. So there's a range of types of products.

When an incident actually occurs or a series of incidents may be occurring, we will also provide steps on how agencies may want to recover from specific types of attacks. We'll set out a checklist so they can actually follow through on how to deal or respond themselves to those incidents.

Hon. Wayne Easter: Mr. Malizia.

A/Commr James Malizia: To your question on how we work with our international partners, of course, if there are threats emanating from another country, we'll work with our vis-à-vis law enforcement agency to be able to further the investigation. Again, in the cyber-world that might be several countries. It might not be just one country.

Hon. Wayne Easter: Then you go through—

● (1220)

The Chair: I'm sorry, Mr. Easter, but you're well over.

Mr. Kerr, for four minutes, please.

Mr. Greg Kerr (West Nova, CPC): Thank you very much, Mr. Chair.

And thank you for attending today.

This is kind of walking on eggshells, this process today. We realize you come in here with some trepidation, because there's stuff you can't share. We appreciate that. But you also understand our need to try to find some consensus on where we're going as well, so we do keep pushing. So I appreciate your caution.

Within that context, in the general generic terms, how do you handle the threats that MPs come forward with? For instance, if any one of us went to you and thought we had a serious issue, could you take us through the steps that would get us through this, as it were?

A/Commr James Malizia: Certainly. Thank you, Mr. Chair.

As you know, ministers of the crown are entitled to receive RCMP protection in Canada and abroad, as needed, by virtue of section 17 of the RCMP regulations. Any threat to a member of Parliament, of course, is investigated by the police of jurisdiction. That may or may not be the RCMP, depending upon the area.

Again, there is a threat risk assessment as this information is received. We have a dedicated team within our national security apparatus that conducts threat risk assessments. It is immediately looked at with respect to protective measures on our protective policing side, where we determine at that point if we should provide preventative security measures. our protective package, while we continue to investigate.

We continue to assess and monitor the situation as the threat is being investigated. Again, security measures will be adjusted according to the process, and ultimately, of course, the investigation will continue with a view and determination to see if there's enough evidence available to charge under the Criminal Code.

Mr. Greg Kerr: Okay. Thank you.

Another major problem I'm sure you must face is that in a democratic country, obviously privacy is a major issue. People are very sensitive about interfering with their businesses, using the Internet, and so on. Is this a major frustration, challenge, or problem for you in sometimes trying to delve into issues that you know are serious issues? Again, I understand this is at a surface level, but the fact that the demand for privacy is there at the same time you're trying to find answers, is that a real challenge?

A/Commr James Malizia: I can say that there are instances where we have the ability to be able to successfully track and identify, and depending upon the complexity there will be times where we will not. Of course, we certainly invite any modern tools and resources to help us respond to the evolving nature of national and transnational crimes.

Mr. Greg Kerr: I realize that's an ongoing change.

On the international front, and again I realize the protection of privacy is absolutely critical for security and a whole lot of other reasons, but in the many contexts you have, with the information flow and so on, do you find a lot of best practices improving because of those contacts? In other words, I'm sure everybody's trying to keep ahead of the curve, so is that an opportunity to really learn new methods, new procedures, or what's going on? I'm trying to be very generic here, obviously. I'm just wondering in a general sense, in the sense of protection for our people, are you learning a lot from other partners around the world?

A/Commr James Malizia: Certainly, we have trusted partnerships around the world that allow us to collaborate together and share on different areas and innovation with respect to best practices.

Mr. Greg Kerr: Okay.

Do you have anything to add, Mr. Gordon?

Mr. Robert Gordon: We have very good sharing agreements with a number of countries. It has proven to be very useful and is very robust, both in terms of best practices at a technical level, but also at a policy level. So as countries are developing cyber-strategies, there are a number of ideas that are coming forward, and that we're sharing aggressively. So it's a very useful process for us.

Mr. Greg Kerr: Okay. Thank you.

That's as deep as I would go anyway, sir.

The Chair: Thank you.

Madam Latendresse, four minutes please.

● (1225)

[*Translation*]

Ms. Alexandrine Latendresse: Thank you very much.

Thank you for being here and for your remarks. What you are telling us is very interesting and it is good to know more about this subject.

Coming back to the case currently before us, we are talking about a video that was posted on YouTube. Can you tell us if there is any way to trace the IP address, for instance, of the person who posted this video online on YouTube?

A/Commr James Malizia: My position does not allow me to give any details about the case you are referring to.

Ms. Alexandrine Latendresse: I mean generally speaking. When someone posts a video on YouTube, is there any way to trace their IP address?

A/Commr James Malizia: As I mentioned at the beginning, there are situations in which we are able to identify individuals on a case-by-case basis. Every case is different and some are complicated. Sometimes we are not able to do so.

Ms. Alexandrine Latendresse: You talked a lot about the threats that can be made against ministers or MPs. I would like to pursue what Mr. Albrecht was saying earlier.

If a minister came to you tomorrow morning with an anonymous handwritten letter containing basically the same type of message—that is, a demand to scrap a bill, otherwise, personal information would be revealed about the minister—would an investigation be conducted?

A/Commr James Malizia: Regardless of the form of the threat received—as an example, of course—we analyze it and, if necessary, we conduct a criminal investigation.

Ms. Alexandrine Latendresse: Whether it is in the form of a letter or anonymous video, an investigation can occur. No major distinction is made in that regard, correct?

A/Commr James Malizia: Are you asking if we would investigate in both cases? Yes, we investigate all cases.

Ms. Alexandrine Latendresse: So the fact that it was a video in this case has no bearing on the importance attributed to the threat.

A/Commr James Malizia: I cannot comment on the present case, but I can say that we would investigate in the cases I described earlier.

Ms. Alexandrine Latendresse: I imagine you have seen the video. Have you seen the video we are talking about and we are supposed to analyze to determine if a breach of privilege occurred?

A/Commr James Malizia: Yes.

Ms. Alexandrine Latendresse: In your opinion, does this video contain any elements that could justify charges? We know that our parliamentary rules were breached, because the video violates a minister or member's right to introduce a bill. But is there anything in the video that could be considered criminal?

A/Commr James Malizia: My position does not allow me to comment on any criminal investigation that is under way.

Ms. Alexandrine Latendresse: Is there anything this committee can do in relation to this situation?

A/Commr James Malizia: We encourage all MPs and ministers to report any threats they receive so we can investigate them.

Of course, our mandate does not address cyber-security. I will therefore refer the question to my colleague from Public Safety Canada, who is here today.

[*English*]

Mr. Robert Gordon: General awareness of what the threats are, or the issues, is a useful thing to try to raise awareness. Public Safety Canada engaged in quite a campaign to do that for Canadians at large. Trying to make citizens aware of what the threats and risks are is a very useful exercise at the preventative or front end of it before incidents actually occur.

The Chair: Mr. Hawn, four minutes please.

Hon. Laurie Hawn: Thank you, Mr. Chair.

Thank you to our witnesses.

Mr. Gordon, you talked about—and Mr. Easter asked you a question about it—the threats to vital systems outside the federal government. In your view, what's the level and what are the trends of those vulnerabilities that we're getting? Are the threats increasing in number? Increasing in severity...? Do we have a grip on it?

Mr. Robert Gordon: We're learning more about the threats every day. One of the things we're actively engaged in is reaching out to the private sector through a variety of forums of the critical infrastructure centre networks that we've established. We're building up the trust within the private sector for them to come forward to talk about the kinds of experiences they have. We're also establishing mechanisms where they can share amongst themselves the types of experiences and the types of cyber-attacks that they're seeing. So they're learning from one another and we learn from them at the same time.

● (1230)

Hon. Laurie Hawn: I want to go back to some comments that Mr. Albrecht made and Mr. Easter commented on as well, as to whether we're talking about this as an individual threat to Minister Toews. I'm going to be asking for an opinion, but in my view it's not just a threat to Minister Toews, it's a threat to the system.

Minister Toews is just a representative of the system doing something that somebody doesn't like, which is the system, not just Minister Toews. In my view, this is a threat to the system of government and not just to an individual minister. Do you have a personal opinion on that?

Mr. Robert Gordon: No, I don't have a personal opinion on that.

Hon. Laurie Hawn: Okay. I'll just lay it out there as my own statement.

Assistant Commissioner, we talked about some of the experiences of other countries, the FBI and so on that have had some limited success in this. Does the RCMP have any experience in similar investigations in recent history, or is this the first one of its kind that you're aware of or can share? I'm not asking for specifics, just are there others?

A/Commr James Malizia: I can say that the RCMP has conducted investigations in the past. We have, as mentioned earlier, a dedicated branch called the technological branch that specializes in this type of area.

Hon. Laurie Hawn: Could you give us any indication of success or not of these other investigations, or are they still ongoing?

A/Commr James Malizia: Of course I don't have any examples for the committee here today, but I can say there have been successful investigations in the past.

Hon. Laurie Hawn: Good.

With regard to a point that Madam Latendresse brought up—whether it's paper-based or electronic-based—extortion is extortion under the law. It doesn't matter whether it's a letter or an e-mail, correct?

A/Commr James Malizia: The RCMP will investigate any variety of those.

Hon. Laurie Hawn: Somebody—I think it was you, Assistant Commissioner—talked about the ignorance of the law. These people don't realize they're breaking the law. So some of them, I guess, may claim ignorance of the law under the influence of their enthusiasm for whatever the cause may be as some level of innocence. Have you run across that sort of attitude? As in, “Gee. I didn't know, so I'm okay. You can't prosecute me.”

A/Commr James Malizia: There have been instances where individuals have provided that as a reason, but also we have seen—and we certainly hope that in those cases where we have sufficient grounds to lay a charge—that it can act as a deterrent.

Hon. Laurie Hawn: Do you think this process we're going through right now—and again, as I've said before, I don't think we have much of a chance of finding these guys. We may find one, but there are who knows how many others.

Do you think that this process is shedding some helpful light for folks out there that this is not a game, that these are crimes, and that ignorance of the law is not going to be treated as an excuse? Has this process been useful at least in that respect?

A/Commr James Malizia: I'm not in a position to comment on the committee's work and the process, but what I can say is that advances in technology have created an environment where individuals achieve anonymity. Criminals exploit, of course, the faceless environment provided by the Internet to conceal their identity and conduct serious criminal activity. We intend to fully pursue those who do that.

Hon. Laurie Hawn: So whether you're a pro or an enthusiastic amateur, the law's going to treat you the same way.

A/Commr James Malizia: Yes.

Hon. Laurie Hawn: Thank you.

The Chair: Mr. Zimmer.

Mr. Bob Zimmer: Thank you, again, for coming today.

We talk about undercover agents in other types of criminal activity. This is a question for Mr. Pickett specifically. Do you have anonymous agents who represent law enforcement to lure out criminals or do you wait for a crime to come to you?

Supt Tony Pickett: I'm sorry. It would be inappropriate for me to comment on a police technique.

● (1235)

Mr. Bob Zimmer: I thought I'd ask.

I also wanted to know about YouTube, and other sites that are utilized—Twitter, and whatever—by different groups. Not necessarily to Mr. Picket, but to any member of the panel, do you have a relationship with these corporations or companies, that if you need access to some of that information due to criminality, you have relationships where they will be forthcoming with information to out the criminal?

Supt Tony Pickett: Again, I can't comment on the relationships we have with businesses regarding techniques that we would use to try to apprehend criminals or criminal activity.

Mr. Bob Zimmer: Okay.

I'd also ask you how you would advise Canadians in general on the use of social media. What would you advise somebody who you consider a friend—and I'm not saying that you don't consider us friends, but it might make it easier to explain—to do in a situation to best protect themselves, I guess, from these attacks?

Mr. Robert Gordon: On Public Safety Canada's website, we actually have some guidance for the public at large, people who are not IT, within an IT department, or within a company or a government department.

We provide that sort of advice to the public on how best to protect themselves.

Mr. Bob Zimmer: Do you have any advice for us today, just off the top of your head—two bits of good advice?

Mr. Robert Gordon: One is making sure your firewalls are up to date. So when the company that you have your firewall with sends you an update, please update it, because that will actually defeat a significant percentage of the attacks that might otherwise go onto your system.

Another is, before clicking on an attachment that comes to you, think about it. We have a saying, “Stop, think before you click.” Is it reasonable that the person who has supposedly sent you this e-mail would send you this attachment? At times, we teach our own staff that. You could perhaps even phone the individual and ask if they sent it before you open it, and that will actually go a long way to preventing a significant number of otherwise successful attacks.

Mr. Bob Zimmer: Sure.

One last bit.

My colleague, Mr. Hawn, has already alluded to this anyway. Deputy Commissioner, I guess you answered it as well. For the rest of the panel, what is the likelihood of catching people who pose threats in the 21st century? Is there a number that you have? Is it likely that they're going to be caught, or what are we looking at?

A/Commr James Malizia: I'm not in a position to provide you with any statistics, but what I can say is that each investigation is unique. Again, in some instances we may be in a position to identify the individuals or individual, and other times we're not.

Mr. Bob Zimmer: I guess, as you've said before, you've had successful investigations where you've caught the bad guy.

A/Commr James Malizia: Yes, we have.

The Chair: Are there any questions? Mr. Albrecht, you have four minutes.

Mr. Harold Albrecht: Thank you, Mr. Chair. I don't think I'll need four minutes.

I don't have a question of the witnesses, but I want to thank them for appearing today, and for their very professional responses. I do want to respond to a statement that was made by Mr. Easter a few minutes ago, when he implied that asking a minister to step down or resign is certainly not a threat. I would agree, but that's much different, Mr. Easter, than threatening to divulge private information about someone if they don't withdraw proposed legislation.

As a former minister of the Crown, I think you should be aware that threatening someone with releasing all private information that may in fact have been secured by devious means, such as hacking into personal accounts, is certainly in a totally different category than simply standing in the House and asking a minister to resign. I would hope that you would be aware of that.

Thank you.

The Chair: Okay.

I have no one else on my list, and we'll thank you for coming today.

Is there anything else for the good of the committee today?

Then I wish you all a very happy Easter, and we will see you when we return.

This meeting is adjourned.

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

On peut obtenir des copies supplémentaires en écrivant à : Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca