Journal of
Military and
Strategic
Studies

VOLUME 14, ISSUE 2, 2012

# *Nobody Knows Anything: Canada's Cyber Insecurities*

This special issue of *The Journal of Military and Strategic Studies* stems from papers presented to the conference, "Nobody Knows Anything: Canada's Cyber Insecurities", held in Calgary during May 2012. The conference focused on Canada, but tackled problems, solutions, conditions and dilemmas which are international. It was hosted by The Canadian Defence and Foreign Affairs Institute; The Centre for Military and Strategic Studies and The School of Public Policy, at The University of Calgary; and The Journal of Military and Strategic Studies. The organising committee was Cam Ross, Major-General ( retired) and Dr. Jack Mintz, of The School for Public Policy; Dr Jörg Denzinger, from The Department of Computer Science, The University of Calgary; and Dr. David Bercuson, Dr. John Ferris and Nancy Pearson Mackie, from The Centre for Military and Strategic Studies. A list of the speakers is attached in Appendix A.

The conference aimed to address complex and important matters, and to recommend policy on them. How was the Internet evolving? What was the nature of cyber security and insecurity, and which actors figured in it? What was the proper relationship between agencies of the state, firms and movements, of society and individuals, in these issues? How should Canada seek to shape this environment, and through what steps in public policy? How should firms, the law and individuals respond to these developments? This collection includes the revised papers presented to the conference, and a thematic introduction. The discussion among 100 academics, business people, systems managers, computer security personnel, lawyers, civil servants, intelligence and military and police officers, and students, occurred under

ISSN : 1488-559X

Chatham House rules, but this introduction will address some of the themes which emerged among them, along with the ideas of the speakers, and our own.

The title for the conference stemmed from the comment of the legendary producer, Sam Goldwyn, that when it came to predicting audience reactions to Hollywood movies, "nobody knows anything". When organizing the conference, we believed that issues related to the Internet and all things "cyber" , were poorly understood, because they were new and complex. The constant repetition of the almost undefinable term "cyber", and its application as a prefix for any activity related to the Internet, showed the mushiness around the matter. These issues involved many activities ( hobbies, business, state security, law and law enforcement, crime, social media, intelligence), techniques and forms of technology, and communities, both users (academics, businesswomen, soldiers, activists, criminals, intelligence officers, lawyers, students, hackers, network managers, lovers of bargains or pornography) and students (computer scientists, sociologists, strategists, politicians and police, techies, geeks and nerds). None of these groups understood all of these phenomena. They rarely interacted as a whole. Only when members of these disparate communities were brought together, we believed, and made to discuss these topics in a context of competitive cooperation, could "cyber" be appreciated in breadth, depth and detail. In order to achieve these aims, this conference sought to combine commentators with different perspectives and expertise, for example, ensuring that every panel included academics, businessmen, and practitioners of computer security and public policy; by having civil libertarians, lawyers and signals intelligence officers, engage each other. We hoped to evoke a serious debate, and to define where we stand regarding these issues in the middle of 2012, while looking ahead as far as possible. These papers, which reflect this diversity of expertise, attest that we achieved our aim.

We asked Dr. John Aycock, an academic specialist in computer security, with an unusual ability to discuss technical issues in plain English, for a blue sky analysis of how the Internet and cyber security might evolve over the next five to ten years. He responded with what he called "wild unsubstantiated assertions" (which others might call, "normal political science"), emphasizing the interaction between social, state, corporate and technological developments. Dr John Sheldon, a student of cyber from a strategic perspective, comprehensively assessed the nature of attackers and targets in that domain, ranking dangers with breadth, precision and balance. States were the greatest dangers in cyber, while criminals were the most common. John Adams, recently chief of The Communications Security Establishment, the signals intelligence agency of the Canadian state, assessed defence against cyber attacks on Canadians, their businesses and civil society, and agencies of the Canadian government. Canada was particularly vulnerable to the danger, given its unusual reliance on the Internet. Harvey Rishekof, a ranking American commentator on the legal and political dimensions of cyber security, provided a comprehensive assessment of these issues. He demonstrated the complexities of the interaction between the interests of states, society and business, and the imperatives of security and business. Finally, Dr. Ron Diebert, who possesses a rare combination of expertise in the politics and technicalities of cyber and the Internet, analyzed all aspects of these issues, and offered recommendations for public policy on them. He emphasized that these matters were above all political, not technical: reflecting the values of societies and individuals, and the aims they hoped to achieve. His paper was commissioned by The Canadian Defence and Foreign Affairs Institute. We reprint it with their authorization, and our thanks.

Surprisingly, given the range of viewpoints expressed at the conference, consensus emerged on several key points, which also delineates the areas of controversy. Insecurity, all agreed, was unavoidable on the Internet, given the way its architecture emerged, software was written, and people used their systems. As ever, the problem with security systems are the people who use them, or do not. Insecurity may be reduced by many means, which wise actors would pursue because that might boost their position, but it never could vanish. Given the classic reciprocity between offence and defence, increased levels of security simply would make attackers raise their game, which they easily could do. If the most powerful states on earth could not protect all of their traffic carried over wireless or the Internet, how could a firm or person do so? Insecurity was not simply a problem, a matter demanding solution, but a condition, something to be endured. It is perhaps best understood as a condition affiliated with problems, not all of which could be eliminated at the same time; or, as the product of an interlocking conglomeration of competitions, between a host of competitors.

Even more, commentators agreed, the danger of cyber insecurity was easy to overstate. There were threats on the net, particularly from the actions of states, including western ones, but simply to securitize these matters, to see them purely or primarily from a military perspective, would be bad for all, including military institutions. Nor were the biggest problems those which seemed most alarming, like cyberwar or cyberterrorism, although these matters could not be forgotten. Well publicized activities like hactivism posed little threat to cyber security. At present, the key problems were cybercrime, and cyberintelligence, whether conducted by, or against, states or non state actors. The issues were great, involving trillions of dollars, the survival of firms and forms of civil liberties, and the success of states. Key parts of the issue concerned intelligence and military agencies, but the core of the problems and solutions lay in politics, both at the international and national levels, involving issues of government regulation, law, law enforcement, and the relationship between individuals, firms, states and societies. The questions of where to define these margins, and which value to emphasise over another, produced disagreements among our audience: not surprisingly, given their significance.

Generally, commentators also agreed that in the summer of 2012, the Internet was changing fundamentally, due not to technology, but rather socio-political forces: the increasing volume of users, especially from non-western countries, and pressures of securitization, corporatization, nationalization and militarization. Some of these pressures were old news. For the first half of their history, so far, computers and computing were driven by the needs of states regarding ballistics and cryptology, with signals intelligence agencies, the dominant consumer, providing the pull—suddenly succeeded by the push of corporations. The military and civil authorities of one nation, the United States, created the earliest versions of the Internet. American society and politics (combined with those of other early users, mostly from liberal democratic countries) stamped the evolution of the Internet, and the international commons it became. Whether in regulation of the Internet, the influence of libertarian values on its evolution, or in the wild west character of its nature, this commons worked on liberal democratic rules. What is new in 2012 is the sheer significance of the Internet to life across the earth, combined with a competition to restructure it, in what might be called the first world wide web war. Many governments see the commons created by liberal democratic states and societies as a threat to them, and a weapon for us. To further their interests, and make us play their game rather than vice versa, these governments deploy their strong suits, state control, and the rapid rise in the number of non-western users of the Internet. Thus, the commons is being divided through a struggle between ideologies, societies and states. How this division and struggle would work is not yet written.  It could take many forms, including cooperation and competition, and international and national regulation. Naturally, other states would pursue their interests against liberal democratic ones, and non-western peoples reconfigure the Internet to suit their concerns. Nor was anything intrinsically wrong with regulation—if governments regulated cars, why not the Internet?  But for Canada, and every liberal democratic country, this process of regulation would be complex, involving all interest groups within their borders, and many without, amidst an international struggle over power and values.

Here emerged a dilemma, which the authors describe in their own words, rather than summarizing expressions garnered under Chatham House rules.

Cyber transforms the roles of communications, intelligence, and information processing, in any human relationship, whether involving government, business, war or love.  Cyber simultaneously dissolves many of the established and dualistic borders which westerners use to demarcate lines amidst state and society, such as between states and societies, internal and external relations, war and peace, civil and military, security and insecurity, and sovereign and non-state actors.  Once, for example, signals intelligence agencies could distinguish between traffic intercepted at home and abroad, so enabling liberal states to combine civil liberties and cryptology. That no longer automatically is true in 2012, when messages surge without human direction between servers at home and abroad, and signals intelligence agencies have an unparalleled ability to read the mail of private citizens, as against foreign states. Once, states fought only each other, and alone controlled the highest levels of violence (part of the problem with terrorists was their claim to act like states, and their efforts to do so). In 2012, non-state actors could use the same techniques (to apply military jargon) of computer network exploitation (CNE, or cyberintelligence) or computer network attack (CNA, or cyberwar) as governments did, and members of either group could apply them against anyone. Once, western legalists could imagine war and peace as being different realms ( though the practice of covert action or political warfare violated this theory, while marxist-leninist and other ideologies denied that distinction). In 2012, however, if a state suffered a cyberattack, one might not know who had launched it.  Foreign states could attack your citizens in time of peace without you knowing the fact or being able to defend them, threatening every conventional element of sovereignty.

Taken together, these developments dissolve another boundary: what Michael Warner calls the difference between sovereign and non-sovereign competitions. In recent history, the restraints imposed by sovereigns distinguished human competitions. Bilateral competitions in business or politics might match the ruthlessness of diplomacy, deploying all means short of war to destroy an enemy, information used as states do intelligence. Non sovereign competitions might be like games of kings, with one exception only, but of weight: war. They had rules enforced by a superior authority, which monopolized the legal use of force, and the collection of intelligence, within its territories.  Rules might be broken, and subjects behave in sovereign forms—murder, espionage—but such behavior was risky business: it could be punished. States, unlike firms, could escalate to war. If a rival beat them at their business, they might kill him. Sovereignty restrained subjects from state practices of intelligence and actions, ensuring that economies were run through open sources, rather than secret intelligence, while the most ferocious political rivalries stopped short of murder. It deterred cheaters, and punished pirates: failure to do so overthrew a sovereign. A central role for the state in any non-sovereign competition, economic or political, was to maintain order, security and certainty, which required a sovereign able to defend rules against any threat: over-mighty subjects, foreign governments—and itself.  Who could more utterly overthrow rules, than their guarantor?

Sovereign restraint, and self-restraint, are fundamental to every non-sovereign competition. A sovereign must maintain rules against all comers, itself included--otherwise, all societies would be totalitarian. The process varies with every case and country, but all share classic tensions. Instrumentality drives subjects up the ladder of escalation, where sovereigns stop an open ended competition for knowledge, power and survival. If they do not, rules change, subjects suffer, sovereignty fails.  Sovereigns confront the temptation to strike downward, resisted by citizens below. Changes in technology, social attitudes or external affairs, drive subjects and sovereign in constant and powerful ways. The state and its agencies must balance the needs for enforcement and restraint, certainty, law, order, security, privacy and liberty,  against subjects -- businesses, private detectives, criminals, activists, terrorists, spouses--  using intelligence and power against each other, or governments;  and also foreign entities interfering in your affairs, or those of your people. Sovereigns must blunt the power of their agencies at home, while keeping them sharp enough for their work. Subjects must keep sovereigns to their task, neither too strong nor weak, but just right, or the competition fails.  Sovereigns confront subjects which ruthlessly—legally or illegally-attack their fellows, states, or the rules and legitimacy of systems. This struggle marks relations between security services, and activists or journalists. Terrorists make war on politics, and attack the systems of sovereign restraint and self-restraint on which the latter rest. Similar tensions affect subjects, in their competitions with each other, and the agencies of the state, in matters like politics, business, and life. Only outlaws, or totalitarians, collect intelligence, and act on it, by whatever means they can.

These tensions are embodied in the law, law enforcement, and regulation, the central competitions where state and subject interact on matters of power, rules and intelligence. Each country assigns different powers for the collection of intelligence to police, prosecutors, judges, defence counsel, and rules for its use as evidence, which address matters like examination for discovery, full disclosure, the powers of interrogation of detectives or magistrates, and the legal use of telephone intercepts, or of what information citizens  might gather on each other, and how. These tensions between sovereign and subjects drive the role of intelligence for states, at home and abroad.

Cyber challenges these characteristics of sovereign and non-sovereign competitions, and entities. With so many players collecting so many forms of information, and giving others access to that material, it is hard for anyone to determine when or whether laws are broken:  or by whom. Internet identities often are issued by non-sovereign players, outside the control of any one state. Identity theft is easy, complicating any determination of who did what to whom, and enabling the creation of artificial players: people acting under pseudonyms or false flags. This diminished likelihood of being caught in illegal or warlike behaviour (or else, the increased ability to pass responsibility for it to others) reduces restraint by any player, and encourages all of them to escalate their own actions, before they know that anything unpleasant is being done to them. Anonymity drives escalation, and the violation of laws and rules by all players, sovereign or otherwise. It complicates retaliation, and therefore any traditional sovereign strategies of policing and deterrence. It reduces the power of calculated defence and increases that of secret attack, for all players in all competitions, and subverts the nature of sovereignty. How can a sovereign maintain order, security and certainty, and defend its subjects, and its own status, against attackers it cannot identify? Meanwhile, traditional decision making systems cannot handle the speed of cyber attacks, forcing sovereigns to enlist non-sovereign and non-human players in defence, or offence. In some competitions, as on the stock market, only automated tools can handle the speed of communication and the volume of information. The interactions between automated systems are as unpredictable, and sometimes as counter-productive, as reciprocal relations among humans. Even worse, key interactions like arbitrage in business and the use of drones in war, combine unique, shifting and instantaneous relations between automated systems and humans, working in specific ways no one has experienced. The number of these interactions surely will rise. Under such circumstances, systems failures are normal—not a problem to be solved, but a condition associated with problems.

The dissolutions of boundaries between sovereign and non-sovereign competitions caused by cyber, produces our dilemma. Sovereign restraint and self restraint are challenged fundamentally in many ways at the same time, as never before. Citizens are threatened by attack from their fellows, and foreign governments and firms, against which they need the aid of their state, which also poses unprecedented problems for civil liberties at home. Canada, and every liberal democratic country, confronts overlapping competitions between groups of competitors, all seeking to defend interests and prerogatives guaranteed under an old order, which emerged after long struggles over power, rules and intelligence. States and signals intelligence agencies wish to behave as they have done for decades, so do lawyers, businesses and activists. For all of them, however, to retain an old status means the need to acquire more power than they had before, and to challenge the position of others. This dynamic forces battles in every country about fundamental issues. When the digits have settled, these boundaries may be reestablished in new ways that seem natural to our children; but reaching that status will be hard. The ideal outcome, a series of highest common denominators, will require tough debate, through which every participant may lose and gain. In key areas, however, no highest common denominator may be possible, forcing tragic choices: to sacrifice one good, in order to maintain another that, somehow and through some means, we rate higher.

Focusing on the main dangers to cyber security—cyberintelligence and cybercrime, rather than the potentially greatest ones, cyberwar or cyberterrorism—simplifies the problem, but even so, it remains powerful. Cyber magnifies the capabilities of intelligence. Before 1914, the techniques of cryptanalysis, the interception of military messages in the field, and the stealing of documents from government offices, were distinct genres of intelligence collection. With the single exception of agencies attacking diplomatic telegrams and dispatches, no one regularly intercepted messages which then were cracked by cryptanalysis. During the first age of signals intelligence, 1914 to 2000, interception and cryptanalysis became integrated, and new disciplines like traffic analysis emerged, but documents and communications intelligence remained distinct. No attacker could read every document scattered through millions of drawers, providing some security to states and far more to individuals. Totalitarian states systematically intercepted the mail and telephone calls of citizens, but these practices were restrained in liberal countries. In the second age of signals intelligence, once state and individual archives went on-line, documents were exposed to attack, just like digital messages and through similar means. Meanwhile, the rise of mobile wireless devices increased the amount of private communication susceptible to interception. Communications intelligence had more range and power than ever before, but potentially was exceeded by cyber intelligence, whether gained by penetrating password protected gateways or through emerging disciplines like "socmint", material garnered from social media. A novel threat emerged, of a nuclear strike on data. One could not merely read the documents in someone's archive, but write them. One corruption of information, producing one failure, might cripple any decision making machine, or the trust on which it relies, or cause a systems failure.

Even more, signals intelligence was a prerogative of states: non-state actors rarely had that capability. Cyberintelligence, conversely, could be practiced by many non-state actors, and far more people were vulnerable to attack than had been true with cryptology. Communications security, once simply a function of states, now mattered to billions of people: in order to help them, a highly bureaucratized and militarized discipline would require transformation. The entry costs to cyber intelligence are small and the payoff large. CNE offers states access to traditional targets of cryptanalysis, and also to private communications and archives which once were unreachable. It offers non-state actors power to collect intelligence they never had before. The targets are easily found, and vulnerable because the social use of communications systems in normal life shapes their application in official capacities. The prevalent modes of communication in 2012 are a cryptanalyst's dream: unprecedented numbers of actors are communication junkies to unparalleled degrees, actively drawing attention to themselves and exposing their secrets, while security is abysmal. Thus, the popular insistence on bringing one's own wireless devices to work, rather than using standard issue, creates dilemmas for corporations or governments trying to maintain security. So too, communications intelligence and cyber intelligence give cybercrime unusual power, and novel weapons, compared to previous criminal practices.

Current technological and academic developments around the Internet amplify these problems. "Clouds", for example, are networks within the Internet that store data and provide the power needed to perform computations on it. They allow access to this material from across the Internet, thus exposing even more information of firms and individuals to third parties, including governments that regulate servers within their jurisdiction which store cloud data (perhaps only for a few seconds). Even worse, if this data is to be processed, the owner cannot even encrypt it, leaving all security to the managers of the cloud. Going further, the idea of the "Internet of Things" assesses equipping matters like appliances in houses or fields, and so on, with sensors, embedded processors and, naturally, Internet connections (usually wireless). Such developments offer further targets for communications and cyber intelligence. Cyber warriors might turn your toaster against you.

At this stage, differences emerged in opinions at our conference. Collectively, they show the complexity of the problems and solutions at hand, and the need for careful assessment so to maximize the discovery of highest common denominators in policy, and to minimize the cost of tragic choices. Decisions must be made on these issues. Whatever actions we take will embody those choices. They will be made through a series of wide-ranging struggles, involving winners and losers. These processes will not be simple: in some cases, supporters of free markets, civil liberties, liberal internationalism and Internet libertarianism, might combine against advocates of national security, with coalitions shifting on other matters. All of these views must be expressed with full force if we are to approach any optima in policy.

The first set of differences involved strategic and political issues of the highest order: how should Canadians, and citizens of other liberal democratic states, respond to the occurring and anticipated division of the Internet? All participants wished this commons could remain one whole. If that aim was impossible, they hoped to maintain as large an international sphere (or interlocking series of national frameworks) as possible, based on the existing Internet and marked by liberal democratic values. One might hope, in the long run, that such a model would attract people caught on other sides, as Radio Free Europe and the world services of the BBC and CBC, among others, shaped attitudes behind the iron curtain during the cold war; but how far this aim could succeed against determined opposition, utilizing all technical means to seal their digital borders, was unclear. Probably, as in the cold war, liberal democratic states can pursue a common system, combining Immanuel Kant's views of a liberal internationalist sphere of peace, the imperatives of civil liberties and free markets, and structures for security, but the devil is in the digits. Through what political means could liberal democratic states achieve these common ends? How would we respond to advanced but authoritarian states, like Singapore, which gave their citizens free access to most of our Internet, but censored small parts of it? or to more censorious states which yet offered their people some access to our domain? What would we do with states which gave their citizens much access to our Internet, but apparently hosted cybercrime, or conducted cyberintelligence and cyberwar against liberal democratic countries, like Russia? Would we treat such actions as a tort, a matter for private litigation, or as a cost of doing business, a matter for police, or one for soldiers? How would we monitor our sides of these disparate borders: metaphorically, would we allow free entry, maintain a border security service, rely on military defences, or combine the three in some way?

Nor can liberal democratic countries alone dictate the outcome. We confront a competition, which we do not control. Foreign states will determine their policy on these matters, act in their own interests and react to any actions we take, making us reshape what we do; and vice versa. When confronting such complex and interlinked issues, and reciprocal and multilateral circumstances, actions easily have perverse consequences.

In particular, Diebert argues, if western nations assign signals intelligence services responsibility for executing their policy for the Internet, and monitoring its borders, they will militarize relationships with other states and their peoples, so reducing the chances to spread our values and attract allies. Moreover, given how cyber has transformed their power, signals intelligence services must behave with more transparency and accountability than they have done before (an argument, incidentally, which siginters now conventionally accept: the key divisions lie over the matter of degree). To further our most fundamental aims, liberal political objectives, at home, abroad, and on the Internet, we must accept a higher degree of cyber insecurity than is technically feasible, knowing that it will damage individuals, firms and national interests. Metaphorically, Diebert favours borders on the Internet with complete freedom of entry, and loose security, with police handling most attacks, and military defences used only as a last resort. Given Diebert's experience in working against authoritarian systems on the Internet, and for liberal democratic ones, his views cannot be taken as naïve: they merit respect from realists.

They also lead directly to a second set of differences on policy. Every liberal democratic country is free to formulate its own policy for the Internet, so making this issue politically complex, though in practical terms they cooperate in many ways. None of them can go it alone. Some give bigger leads than others. The United States already has given its signals intelligence agency much responsibility for cybersecurity and monitoring of external threats on the Internet, with the rest assigned mostly to the FBI, a federal agency in charge of internal security and policing. Canada, and many other western countries, have taken similar, though not identical, steps. Metaphorically, they are choosing an Internet which seeks somehow to combine free entry with firm border security, overseen at the frontier by signals intelligence and police, with military forces intentionally left visible, as a deterrent, even though cyber deterrence actually is hard to execute.

Western governments are not taking these steps for trivial reasons. For any state, the greatest threats in communications and cyber intelligence to its agencies, firms and people, come from other governments. These threats exist. They can be countered only by a peer. Canada is part of the greatest signals intelligence effort at work today, through the "five eyes" coalition with Britain, Australia, New Zealand and the United States. This status has concomitants. Canadian policy on signals intelligence and cyber is linked to that made in Washington, unless we break with the "five eyes", at costs no government in Ottawa ever is likely to accept. In judging these issues, one must avoid paranoia. Signals intelligence is a normal activity for states, no better or worse than any other form of intelligence or security, merely more secret; nor is secrecy a sin. Signals intelligence agencies are legalistic bodies, which obey governments: the problem is not that they are rogue elephants, but, rather, that they increase the power of their masters, in ways the latter come to take for granted. So too, cyberintelligence is here to stay, while no nation can ignore cyberwar. The United States has created a military command to conduct cyberwar both offensively and defensively, as many other countries have done. The United States and Israel have conducted cyberwar against Iran. The Russian and Chinese states probably also have conducted cyberwar, through their opaque links to "patriotic hackers" and cybercriminals.

Defence against such matters is unavoidable in a world filled with hungry and hostile rivals, some of which attack the interests of Canada, and of Canadians. The Ghostnet investigation demonstrated how a cyberintelligence effort based in China attacked foreign governments, businesses, and non-state actors across the globe, incidentally threatening firms and civil liberties in Canada. Seemingly well sourced claims from *The Wall Street Journal* claim that Nortel, once central to Canada's presence in high technology industries, collapsed in part from cyberintelligence conducted by Chinese companies, and that Lieutenant Jeffery Delisle, presently under arrest in Halifax, stole military intelligence on a Wikileaks scale from "five eyes" sources for Russian espionage. John Adams defines the scale of the problems Canada faces in theses spheres, and shows that they must be addressed.

At our conference, classic differences also emerged on a third set of issues, the relationship between intelligence, state, society and civil liberties, but with new twists. How, to take but one example, can one correlate old procedures for collecting information through telephone intercepts on matters of criminal justice and internal security, with the new ones required to address social media? On their own, such problems are not new: liberal states have faced them since 1914 and found ways to balance conflicting ends. This balance, admittedly, has accompanied a rise in the power of the state compared to society. By liberal standards of 1912, every liberal democratic country of 2012 is a police state. Intelligence services, however, merely have been one factor in this process, far less significant than matters which many think innocuous, like the rise of the welfare state, information processing and bureaucratized government.

Today, cyber transforms the daily interactions of people with their government, foreign ones, and individuals across the world. The normal threat to security is cybercrime, and other people. The mass of material carried on cellphone and computer networks, and their vulnerability to penetration, creates new targets, attackers, and challenges. Non state actors in non-sovereign competitions are greater targets than before, and better able to strike. Hackers and retired veterans provide expertise to people ranging from criminals to political activists. In 2010, Sea Shepherd used forms of communications intelligence and deception (mounted through Facebook) in its attempts to defeat Japanese whalers in the Antarctic Ocean. Standards for privacy and surveillance are unclear, given the remarkable willingness of people to advertise themselves to the world. Scandals are constant. Celebrities are a greater target than statesmen. For decades around 2000, some British newspapers relied heavily on hacking into cellphones and computers, to gather scoops, which gained their masters political power in London. In search of stories, they penetrated the communications of intelligence officers. They acquired as much communications intelligence on British politicians as any hostile intelligence service ever had done, and embarrassed royalty in ways which would have made heads roll, four centuries before. Preventing hell from being other people in the age of cyber will tax the imaginations of legislators, policemen and journalists. Even most Internet libertarians will accept the need for a police presence in cyber.

For civil society, however, the biggest threats to cybersecurity are foreign governments, and its own. The history of communications since the rise of the printing press links government decisions about national development and security, to freedom of thought and expression for individuals. In the age of cyber, these matters have merged in an uncomfortable fashion. Early advocates of the Internet hoped that it would boost liberal and libertarian aims, enabling freedom for free. In 2012, the forecast is more depressing. The combination of cyber and CCTV enables an Orwellian outcome, that can be resisted only by political will. The problem of sovereign restraint and self-restraint takes new forms. However, the matter is so obvious and important, that a highest common denominator outcome is probable.

A fourth area of difference emerged at our conference over perhaps the most complex, and novel, set of problems produced by cyber: regarding the relationship between intelligence, business and states. For their own purposes, modern western firms wish to minimize government regulation, or interference in the market. They also want wide room to exploit the Internet, and free access across whatever borders may emerge on it. This ambition exposes them to cyber attack from actors at home and abroad. The normal threat is cyber criminals, who seem able to damage business more than anyone before who ever robbed with six gun, or fountain pen. To this danger may be added the actions of other businesses. Although firms and markets, among other things, are systems to process information, businesses typically have not collected intelligence through the sophisticated and intrusive means adopted by states, which are illegal in non-sovereign competitions. Over the past decade, however, evidence suggests that firms, facing opportunities opened by incompetent security and uncertain legality, are collecting illegal intelligence more than ever before, usually working through freelances, like private detectives, unconstrained by corporate loyalty. The cases of Hewlett Packard and News International, among others, show that western firms sometimes collect communications intelligence systematically, so to gain competitive advantages against rivals. Much evidence suggests that firms in non-western countries, perhaps working with their governments, have done so through cyberintelligence.

The greatest threat of cyber attack to any business is a foreign firm working with its home government, borrowing the latter's resources of signals intelligence, to collect competitive and technological information. Though the intelligence services of states do not centre on commercial matters, they have strength there, and reason to exercise it. States enter markets because economics and power are related, while sovereign and non-sovereign competitions overlap, as do claims of sovereignty. Whenever a state aids, or attacks, any economic actor, the competition combines market and power politics. Such intervention is common. Many states think of economics as war. It is power. During the cold war, states routinely acquired commercial and technological intelligence from foreign businesses, used to aid themselves, or national firms, and also helped the latter to improve their security. Since 1989, as power turned on economics and innovation, the attack against and defence of technology became increasingly important. Firms, even more than states, are the target of attack, and more than ever before, their initiator. Coordination with firms has become central to the security and counter intelligence organs of the state, and those functions harder than ever. Offence is stronger than defence, because states and firms may launch wide ranging and coordinated attacks, against targets dogged by inertia and conflicting interests between bureaucrats and businessmen. States must protect their own firms, and people, from foreign cyber attack, and regard such actions as directed not just against one of their subjects, but themselves.

Here emerges a direct clash between the principles of national security and free markets. If firms need government aid against foreign attack, massive regulation and interference will be required, with no clear end in sight. Nor can the old practices and principles for defence of communications by states, militarized and bureaucratized as they are, easily be recalibrated to fit these circumstances. These actions also challenge the patterns of competition and responsibility which underlie the free market system. The easiest way for firms to learn the necessity of cybersecurity is to see the costs, in the slumping values of stock, the firing of CEOs, and the collapse of businesses. Nor is much effort required to make some gains in this area. Good communications and cyber security actually offers firms more of a comparative advantage than it does states. Opportunistic attackers, including most cybercriminals, reach for low hanging fruit, and therefore can be deterred by marginal improvements in security. Serious attackers determined to strike a specific target, conversely, will escalate their scale of attack in response to developments in your defence. The history of cryptanalysis and cryptography is one of constant escalation of power and quality on both sides, with a competitor . Hence, for firms as with states, paranoia is unavoidable: if someone wants to get you, they can try and they will succeed, sometimes. In any case, to reduce the incentives for firms to take cybersecurity seriously will matter: ironically, for a state to protect its nation's firms against foreign attack may weaken their capabilities as businesses. In this area, to find highest common denominator compromises will be especially complex.

Nor does this end the story. The ease of communications intelligence and cyber intelligence will transform the normal collection of information by firms, through legal and illegal means, at home and abroad, and also erode the boundaries between these two latter categories. Businesses have evolved their own unique modes to collect information, distinct from those of states. One subtle and integrated form of interrogation, for example, exploits the fact that firms must outline their capabilities and intentions to many people within their own organization, supply chains, customers, academic and government authorities, spreading news wholesale while possessing primitive security. Again, documents cannot legally be stolen from within offices, but might be taken on the street if tossed with the trash, through the source of garbology. In cyber, any firm gathering megadata from social media may be acting through legal means: but where will the legal line be drawn regarding collection? and who will decide what it is? Here, conflicts of interest emerge between businesses, and society, which only a state may arbitrate and police.

Where precisely to draw the balance between these contradictions in Canadian policy toward cybersecurity and the Internet, is unclear. The time has come to debate them. Metaphors have not yet materialized. Final decisions have not yet been taken, and highest common denominator compromises on details may prevent tragic choices. This will require hard, thorough and transparent work. It ranks high among the issues of public policy facing Canadians, and citizens of all liberal democratic countries.

Jörg Denzinger

John Ferris

APPENDIX A

**Conference Presenters**

Dr. John Aycock, Department of Political Science, University of Calgary

Dr. Ron Deibert, Canada Centre for Global Security Studies and Citizen Lab, Munk School of Global Affairs, University of Toronto

Dr. Harvey Rishikof, Chair of the American Bar Association's Standing Committee on Law and National Security

Dr. John Sheldon, School of Advanced Air and Space Studies, Air University, Maxwell AFB

John Adams, Former Chief, Communications Security Establishment Canada

Rod Howes, Defence Research and Development Canada

John Millar, Digital Boundary Group

Dean Turner, Symantec

Dr. Michael Locasto, Department of Computer Science, University of Calgary

Gillian Stacey, Davies Ward Phillips and Vineberg LLP

John Proctor, CGI

Robert Dick, Department of Public Safety/National Cyber Security