Canadian Radio-television and Telecommunications Commission
Conseil de la radiodiffusion et des télécommunications canadiennes

Compliance and Enforcement and Telecom Decision CRTC 2022-170

PDF version

References: 2021-9, 2021-9-1

Ottawa, 23 June 2022

Public record: 1011-NOC2021-0009

Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety

The Commission finds that regulatory action is necessary to ensure that Canadian carriers that block botnets do so in a way that provides a baseline level of protection to Canadians.

The Commission establishes the overarching guiding principles for a future network-level botnet-blocking framework and requests that the CRTC Interconnection Steering Committee (CISC) examine a number of issues to assist in developing the technical parameters that are consistent with these guiding principles, and produce a report detailing its recommendations within **nine months** of the date of this decision. Following receipt of the report from CISC and comments from interested parties, the Commission intends to establish the minimum standards for botnet-blocking.

Background

1. On 13 January 2021, the Commission issued Compliance and Enforcement and Telecom Notice of Consultation 2021-9 (the Notice of Consultation), in which it solicited comments on the development of a network-level blocking framework to limit botnet[1] traffic and strengthen Canadians' online safety.

2. Botnets are an integral part of the communication infrastructure used by cyber threat actors. They facilitate a broad range of harmful online activities including the most egregious violations of Canada's anti-spam legislation (CASL).[2] They impact

[1] A botnet is a network of malware-infected devices controlled as a group without the knowledge and consent of the device owners, and toward some malicious end. Botnet traffic is the Internet traffic that flows between infected devices, known as bots and their points of control, known as command and control servers. The use of the term botnet in this decision and in the Notice of Consultation only refers to malicious botnets causing harm to Canadians and does not include distributed processing systems or so-called good bots programmed to perform helpful tasks (e.g., commercial bots and web crawlers).

[2] *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the*

everyone, from large, medium, and small businesses to schools, hospitals, and citizens. They enable spam, distributed denial-of-service attacks, malware deployment, and information theft, as well as giving attackers unfettered access to networks via infected systems.

3. Of particular concern to Canadians are the increasingly common ransomware attacks that have caused significant service disruptions and financial damages. Botnet communication flows through telecommunications service providers' (TSPs)[3] networks. TSPs are therefore uniquely positioned to implement network-level blocking to disrupt harmful botnet activities.

4. The Commission received interventions from individuals and from Allarco Entertainment 2008 Inc.; Bell Canada; Bragg Communications Incorporated, carrying on business as Eastlink (Eastlink); the Canadian Internet Registration Authority (CIRA); a joint submission from CIBC [Canadian Imperial Bank of Commerce] and a number of major banks, including BMO Bank of Montreal, Canada Life, Desjardins, Manulife Bank, RBC [Royal Bank of Canada], Scotiabank, and TD Canada Trust (hereafter, CIBC et al.); Cogeco Communications inc. on behalf of its subsidiary Cogeco Connexion inc. (Cogeco); the Communications Security Establishment (CSE);[4] a joint submission from Crypto Québec, Hackfest Communication, and INFOSECSW (collectively, INFOSECSW); the Digital ID & Authentication Council of Canada; Distributel Communications Limited (Distributel); Electricity Canada;[5] the Independent Telecommunications Providers Association and the Canadian Communications Systems Alliance (ITPA/CCSA); the Internet Society; Lumen Technologies, Inc.; the Manitoba Coalition (composed of the Aboriginal Council of Winnipeg, the Manitoba Branch of the Consumers' Association of Canada and Harvest Manitoba);[6] the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG); Nokia Canada Inc. (Nokia); Open-Xchange AG; the Public Interest Advocacy Centre (PIAC); Quebecor Media Inc., on behalf of Videotron Ltd. (Videotron); Rogers Communications Canada Inc. (RCCI); the Royal Canadian Mounted Police (RCMP) National Cybercrime Coordination Unit; the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC); Saskatchewan Telecommunications (SaskTel); Shaw Communications Inc. (Shaw); Stealth Network Services; TekSavvy Solutions Inc. (TekSavvy); TELUS Communications Inc. (TCI);

Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23 is commonly referred to as Canada's anti-spam legislation, or CASL.

[3] The term "TSPs," defined in the *Telecommunications Act* as persons that provide basic telecommunications services, refers both to facilities-based providers and resellers, and includes Internet service providers.

[4] The CSE is the technical authority for cyber security in Canada and the operator of the Canadian Centre for Cyber Security (CCCS).

[5] Electricity Canada used to be known as the Canadian Electricity Association. Its interventions as part of this proceeding were made under that name. It changed its name to Electricity Canada in early 2022. For ease of reference, Electricity Canada is used in this decision.

[6] The Manitoba Coalition conducted two consumer engagement sessions in the context of the Notice of Consultation and reported the views of various individuals in its submission.

Vaxination Informatique; and Xplornet Communications Inc. and its subsidiary Xplore Mobile Inc. (Xplornet).

Requests for information (RFIs)

5. Commission staff issued RFIs to the TSPs that intervened in the Notice of Consultation, namely Bell Canada, Cogeco, Distributel, Eastlink, RCCI, SaskTel, Shaw, TCI, TekSavvy, Videotron, and Xplornet.

6. Given that the interventions the Commission received from TSPs suggested they already have measures in place to mitigate botnet traffic and, in certain cases, remediate associated malware infections, the purpose of the RFIs was to understand the scope of TSPs' existing anti-botnet activities. They were also aimed at ensuring that additional information about the nature, scope, and conditions of the botnet blocking performed to date by TSPs was included by TSPs on the public record.

7. All of the TSPs listed in paragraph 5 filed responses to the RFIs.

8. The Commission received replies to the RFI responses from six parties: Marc Nanni, Bell Canada, RCCI, TCI, TekSavvy, and Vaxination Informatique.

9. The public process closed at the end of the RFI reply period, on 12 August 2021.

Issues

10. The Commission has identified the following essential issues to be addressed in this decision:

    - Does the problem of botnet traffic necessitate regulatory action?
    - If the problem of botnet traffic necessitates regulatory action, what kind of regulatory action would be appropriate?
    - What are the technical parameters of a blocking framework?

Does the problem of botnet traffic necessitate regulatory action?

The scope of the problem posed by botnet traffic

The Commission's position in the Notice of Consultation

11. In the Notice of Consultation, the Commission outlined why botnets and botnet traffic are a problem. Malicious cyber activity targets Canadian consumers and businesses, as well as organizations that provide critical services, such as hospitals, schools, and government bodies. This malicious activity compromises privacy and impairs network integrity and availability. It also imposes costs on the victims and undermines Canadians' confidence when they use electronic communications to carry out their online activities.

12. These activities commonly leverage botnets to provide an attacker with access to private networks while maintaining the attacker's anonymity. Of particular concern to Canadians are frequent ransomware attacks, which have caused significant service disruptions and financial damage.

Positions of parties

13. The majority of parties agreed that botnets continue to be a significant cyber security[7] issue both in terms of traffic volume and severity of harm. CIBC et al. and SaskTel submitted that they estimate malicious bots account for 20% to 30% of all Internet traffic, and added that these bots have already caused significant harm to the economy and national security. SaskTel added that botnet traffic is undesirable for those who manage networks.

14. Distributel submitted that botnets continue to be a global problem despite significant resources allocated to addressing them.

15. The Internet Society submitted that Canadians are increasingly in need of solutions to address botnet activity and broader trends in cyber-attacks, particularly during the COVID-19 pandemic, because a great proportion of daily activities take place online.

16. PIAC submitted that botnets infringe on Canadians' fundamental right to privacy, threaten jobs, and shatter the public's trust in online services.

17. Notwithstanding changes in online behaviour brought about by the pandemic, Nokia submitted that fifth-generation networks and the proliferation of Internet of Things devices means that botnet attacks are likely to be much larger and more powerful if left unchecked.

18. Bell Canada, RCCI, and TCI agreed that malicious botnets are causing harm to Canadians but questioned their prevalence.

19. While Bell Canada, RCCI, and TCI submitted, in their responses to the RFIs, that they consider cyber security to be a priority, they added that the percentage of their networks' traffic that they attributed to botnets or malware over the past five years is not available. Bell Canada, RCCI, and TCI referenced Xplornet's very low percentage (0.0002 %) to support their argument that there is no evidence of a problem justifying regulatory intervention.

---

[7] Cyber security means the body of technologies, processes, practices, and response and mitigation measures designed to protect against cyber attacks and ensure confidentiality, integrity, and availability of electronic information. A cyber attack is the use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

Commission's analysis and determinations

20. The Commission notes that the majority of parties considered that botnets constitute a significant cyber security issue. This view is supported by the academics and cyber security specialists who intervened in this proceeding, and aligns with the policy position taken by regulators and governments in countries around the world, including Australia, Finland, Germany, Japan, the Netherlands, Norway, South Korea, the United Kingdom, and the United States.

21. While a few parties submitted that botnets are not a significant issue, the following factors suggest otherwise:

    - The statistics provided by Nokia give a global view of device infections. The Commission considers that there is nothing to suggest the numbers in Canada would be significantly lower or higher than the global numbers. Nokia's global statistics can therefore provide additional insight into the scope of the issue within Canadian mobile device and broadband subscriptions. Nokia measured a monthly mobile device infection rate of between 0.2% and 0.5% between 2017 and 2020. Combined with Canadian smartphone usage data, this suggests there could be between 61,000 and 153,000 infected mobile devices in Canada in any given month. Nokia showed that the number of Internet-connected households with an infected device decreased between 2017 and 2020. The fixed residential network infection rates of 6% to 3.2% for the 36-month period between 2017 and 2020 identified by Nokia translates to a total number of Canadian households with at least one malware-infected device ranging from 910,000 to 485,000 over the course of that period.
    - The estimates referenced by CIBC et al. and SaskTel suggest botnet traffic represents 20% to 30% of total Internet traffic.
    - The projections based on market shares for 8 out of 11 participating Canadian TSPs (Bell Canada, Cogeco, Eastlink, RCCI, SaskTel, Shaw, TCI, and Videotron) for the first quarter of 2021 suggest that Canadians or devices in Canada are attempting to access malicious domains at a rate of about seven million per day.

22. The Commission recognizes that malicious websites accessed by Canadians as a percentage of total websites visited may be low in absolute terms. However, since visiting a single malicious domain is sufficient to advance a device infection or result in credential theft, the Commission considers that even the relatively small ratio detected by TSPs is significant.

23. In light of the above, the Commission concludes that botnet traffic constitutes a significant issue for cyber security, both in terms of volume and severity of harm.

Is regulatory action necessary?

The Commission's position in the Notice of Consultation

24. In the Notice of Consultation, the Commission invited feedback on the appropriateness and effectiveness of the existing regulatory mechanisms to address the harm caused by botnets.

Positions of parties

Parties in favour of regulatory intervention

25. Although their specific views differed in scope, a number of individual interveners as well as CIBC et al., CIRA, the CSE, Electricity Canada, the Manitoba Coalition, Open-Xchange AG, PIAC, the RCMP, SaskTel, Shaw, TekSavvy, and Videotron all supported regulatory intervention by the Commission. The support from these parties stemmed from a recognition of the persistent and criminal nature of botnets, as well as from the increasing prevalence and negative impact of botnets on the Canadian economy.

26. The CSE, Electricity Canada, and the RCMP all agreed that blocking by TSPs would help to address cyber threats faced by Canadians and diminish Canadians' exposure to associated risks. CIBC et al. submitted that it is Canadian consumers who face the majority of risk when it comes to losses through fraud, including fraud perpetrated via botnets. Large corporations have the skill sets and resources to react to botnets and cyber-attacks, whereas citizens often do not. Dr. Benoit Dupont, the Manitoba Coalition, and Open-Xchange AG characterized the challenges faced by citizens by arguing that the sophistication of botnets makes them resilient to mainstream antivirus and other removal tools available to end-users, and that end-users often lack the skills to understand the risks presented by botnets.

27. TekSavvy was initially opposed to regulatory intervention and claimed that network-level blocking would be ineffective and inappropriate, and that it would break the Internet. It later reversed its position based on the interventions submitted by other TSPs, which indicated that most have already been blocking botnets and other cyber threats for many years. In its final reply, TekSavvy submitted that the RFI responses confirmed and amplified the clear need for independent and principles-based oversight of the blocking activities widely undertaken by TSPs. TekSavvy called on the Commission to establish a lightweight incentives-based framework.

28. CIRA, PIAC, and TekSavvy argued in favour of regulatory intervention given that TSPs are already blocking malicious traffic but, in their view, doing so without the authorization required from the Commission under section 36 of the *Telecommunications Act* (the Act). CIRA defended the TSPs' blocking activities by arguing that the Internet ecosystem includes malicious traffic that would prevent the Internet from functioning if left unaddressed. It concluded that the Commission should grant TSPs limited permission to block malicious traffic.

29. Parties in favour of regulatory intervention and neutral parties highlighted the lack of information regarding TSPs' current practices. For example, CIPPIC refrained from commenting on the need for regulatory intervention in part because the current blocking practices of TSPs are largely unknown. The Manitoba Coalition submitted that some participants in the focus group it led, especially the senior population, seemed to think that botnet traffic blocking was already systematically implemented by TSPs.

30. Though PIAC submitted that some level of Commission intervention may be appropriate, it noted that such intervention presents potential harms to net neutrality. The Manitoba Coalition suggested that an exception to net neutrality may only be acceptable if it is narrowly constrained to its intended purpose, minimally intrusive, highly responsive, and effective.

Parties opposed to regulatory intervention

31. Individual interveners, Bell Canada, Eastlink, INFOSECSW, the Internet Society, the ITPA/CCSA, RCCI, TCI, and Xplornet argued that regulatory intervention is unnecessary. In particular, Bell Canada, RCCI, and TCI rejected the idea of a mandatory blocking regime. The parties opposed to regulatory intervention argued that the existing flexibility afforded through collaboration is more adaptable than regulation, that a regulatory authority to block botnets already exists, that the current blocking efforts already follow industry best practices, and that other parties can contribute to botnet mitigation strategies more than TSPs can.

32. According to Bell Canada and RCCI, several TSPs (Bell Canada, RCCI, SaskTel, Shaw, TCI, and Videotron) are already sharing botnet and malware indicators of compromise (IOCs)[8] through the Canadian Security Telecommunications Advisory Committee's (CSTAC)[9] sub-working groups and other forums.

33. Dr. Fenwick McKelvey and Dr. Reza Rajabiun (in a joint intervention), Bell Canada, and RCCI submitted that the status quo (i.e., TSPs deal with botnets and malware by liaising with each other, government departments, and law enforcement officials) is working well and that the current mechanism need not be augmented. The Internet Society and TCI agreed that cooperation is the proper way to address botnets but added that the botnet problem would benefit from broader collaboration.

---

[8] An IOC is a piece of forensic data, also known as an artifact, observed on a network or in a computer system that indicates, with high confidence, intrusion on that system and, more broadly, that malicious activity is occurring. In other words, IOCs are identifiers related to cyber-attacks. Typical IOCs are virus signatures and IP addresses, MD5 [Message Digest 5] hashes of malware files, and Internet addresses or domain names of botnet command and control servers. Security researchers use IOCs to better analyze a particular malware's techniques and behaviours. IOCs also provide actionable threat intelligence that can be shared within the community to further improve incident response and remediation strategies.

[9] CSTAC is an advisory committee that allows the private and public sectors to exchange information and collaborate strategically on current and evolving issues that may affect telecommunications infrastructure, including cyber security threats. CSTAC includes the Canadian Telecommunication Cyber Protection Working Group, which has developed best practices for Canadian TSPs.

34. The parties opposed to mandated regulatory intervention also argued that a formal framework is unnecessary since the current regulatory environment permits network-level blocking of security threats such as botnets. However, parties relied on different regulatory mechanisms to support blocking. Most parties, both those opposed to mandated regulatory action (e.g., RCCI and TCI) and those supportive of it (e.g., CIBC et al. and Shaw), were of the view that in Telecom Regulatory Policy 2009-657, the Commission permitted TSPs to block botnet traffic at the network level.

35. Bell Canada stated that it is unclear whether the Commission has the requisite authority, either under CASL or the Act, to implement a mandatory botnet blocking regime. Further, it submitted that CASL expressly allows TSPs to alter transmission data, and thereby block traffic for network management purposes.

36. Another factor put forth by the parties opposed to regulatory intervention was the current use of telecommunications industry best practices such as those from the Broadband Internet Technical Advisory Group (BITAG), CSTAC, and the Internet Engineering Task Force. The parties claimed that these best practices already provide the necessary recommendations to implement botnet blocking.

37. Xplornet expressed its concern that a botnet-blocking framework would cultivate a false sense of confidence among Canadians and other non-TSP stakeholders, leading them to believe that Canadians are fully protected against malicious online activity and do not need to exercise good cyber hygiene. Similar concerns expressed by other parties opposed to regulatory intervention suggested that other entities can better contribute to a botnet mitigation strategy, particularly

    i. end-users, who can use existing solutions to secure their devices and their Internet connection (security updates, antivirus and firewall paid solutions provided by TSPs and security vendors, the CIRA Canadian Shield[10] program, etc.);

    ii. other providers in the Internet ecosystem, such as device manufacturers (e.g., Internet of Things device manufacturers) and software vendors, who can ensure that they do not sell products with outdated or weak software;

    iii. the federal government, which can regulate the other providers mentioned in paragraph 37(ii) and support user education to prevent bot infections from occurring in the first place; and

    iv. law enforcement agencies, which can develop international cooperation networks to tackle botnets at their source.

---

[10] CIRA Canadian Shield is a network-level blocking mechanism provided as a collaboration between Akamai Technologies, the CCCS, and CIRA. It is a domain-based blocking service offered free of charge to all Canadians, on an opt-in basis. Users opt in by configuring their router to send domain lookups to CIRA's resolver.

38. Parties opposed to regulatory intervention, including Samuel Harper, Karine Leduc, Marc Nanni, and INFOSECSW, argued that this project will harm, or clearly go against, freedom of expression and the principle of net neutrality recognized by the Commission.

RFI responses

39. Throughout their submissions in this proceeding, most TSPs either implicitly or explicitly responded that they collaborate with one another and have specific blocking systems in place to address malware and spam.

40. In addition to the information submitted in confidence by TSPs, Shaw and Xplornet submitted that they also use automated methods to share botnet IOCs. Shaw added that it shares IOCs with CSTAC and the Canadian Centre for Cyber Security (CCCS), but Xplornet indicated that it only shares IOCs with unnamed interconnected TSPs once daily. Videotron submitted that it plans to automate its sharing but did not provide a timeline. Cogeco, Distributel, and TekSavvy submitted that they do not share botnet IOCs. Cogeco clarified that, on detection, it sometimes shares IOCs related to phishing, malicious domains, or other cyber threats with any concerned stakeholder, including software and/or hardware developers, on a manual or ad hoc basis.

41. All TSPs, with the exception of Cogeco, Distributel, and SaskTel, provided responses suggesting they currently block botnet traffic. Shaw clarified that its blocking options are not made available to the subscribers of its Freedom flanker brand.

42. Eastlink submitted that it uses a third party blocklist to detect and block botnet traffic on its domain name server infrastructure. RCCI submitted that it uses a proprietary blocking system but did not specify what method(s) it uses. Shaw outlined its three different blocking systems: (i) a free opt-in domain-blocking service that leverages a third party blocklist; (ii) a fee-based end-user solution sold as an add-on to block unauthorized access attempts; and (iii) a fee-based security solution for its small- and medium-sized business customers that includes domain filtering and an antivirus solution.

43. TSPs also identified a number of different third parties that they use to monitor traffic and facilitate blocking or customer notifications. The third parties' blocklists identified by TSPs varied, but all included a broader range of IOCs that accounted for more than just botnets. The cost of subscription to these blocklists also varied.

44. In reply to the RFI responses, Jonathan Curtis stated that TSPs have a long history of filtering and blocking spam, going back to 1996. Marc Nanni expressed concern regarding the use of third parties' blocklists and added that RCCI, Shaw, and Videotron each use United States-based Comcast X1/Xfinity for third party blocking. Marc Nanni also referenced publications showing Shaw's use of Zvelo and Bell Canada's use of a blocking solution called Bell-Environics.

Commission's analysis and determinations

45. The Commission considers that regulatory action is needed because

- TSPs' current practices are diverse and opaque and lack a practical and consistent mechanism for sharing botnet IOCs;
- TSPs are uniquely positioned to address botnet activity;
- network-level blocking is effective and appropriate; and
- there is confusion among the parties regarding the regulatory basis for the existing botnet blocking conducted by TSPs.

TSPs' current practices are diverse and opaque and lack a practical and consistent mechanism for sharing botnet IOCs

46. While parties opposed to regulatory intervention relied largely on existing voluntary sharing practices and collaboration, TSPs' RFI responses provided no evidence of a practical or consistent mechanism for sharing botnet IOCs in the TSP community. Only a few TSPs are sharing botnet IOCs. In these limited instances, sharing typically occurs in a manual and ad hoc fashion.

47. The Commission recognizes the necessity for collaboration through working groups like CSTAC or CSTAC's Canadian Telecommunication Cyber Protection Working Group. These are essential forums for sharing intelligence on trends and discussing general strategy, architecture, and specific operational or policy matters. However, the Commission considers that this type of cooperation is insufficient for sharing botnet or malware IOCs. IOCs are highly dynamic and the informal transfer of IOCs on an ad hoc basis is neither effective nor efficient. An IOC may even become outdated before the working group session ends. Fast-flux techniques[11] employed by botnets can map a domain to thousands of Internet Protocol (IP) addresses that change second by second. Modern botnets can also use domain generation algorithms to generate near-infinite lists of possible command and control domains. These and other techniques mean a high degree of automation is necessary for the IOC lists to be updated and applied consistently and in real-time by the entire TSP community.

48. In addition, almost every aspect of TSPs' blocking activities differs across the industry. Different TSPs block different threats, using different methods and blocklists. Consistent with the CSE's recommendation, there is heavy reliance on lists that detect a broader spectrum of IOCs (i.e., not only botnets but also spam and malware, whether distributed by botnets or not). There are also examples, like Shaw's BlueCurve, where subscribers who opt-in to blocking must consent to certain forms of content blocking, such as websites considered to infringe

[11] Fast flux consists of swapping IP addresses in and out of Domain Name System records at an extremely high frequency.

copyright, as a condition for blocking for security purposes. TSPs block botnet traffic using either proprietary or differing third party blocklists but rely on third parties chosen at their own discretion. The threat-intelligence organizations responsible for developing and maintaining third-party blocklists are exclusively non-domestic and predominantly United States-based. TSPs did not provide details on whether blocklists are accredited to ensure robustness or audited to assess effectiveness over time. It is unclear whether the blocklists being used are effective at preventing access to infected devices located in Canada.

49. While the Commission acknowledges that variability has its advantages, it also considers that Canadian Internet subscribers would benefit from a solution that provides a baseline level of security and blocks threats targeting Canadians. The most notable Canadian-based solution is CIRA Canadian Shield. Canadian TSPs did not identify CIRA Canadian Shield as one of the solutions they use.

50. The TSPs argued that their blocking methods follow best practices, but the Commission notes a number of inconsistencies. The most notable departure from the best practices is in how TSPs track and categorize blocking events. The CSTAC best practices recommend tracking blocking events and classifying associated infection types, and section 4 of the Internet Engineering Task Force Recommendations for the Remediation of Bots in ISP Networks, RFC 6561 highlights reasons why these activities are critical to addressing botnets.[12] However, the RFI responses demonstrated that most of the responding TSPs do not track blocking events. Among the TSPs that indicated that they track infections, only one TSP claimed to classify them.

51. While the CSTAC best practices policies provide significant and valuable guidance on securing critical communications infrastructure, the Commission notes important gaps, for example,

- the CSTAC best practices do not specify standards that must be met to achieve the objectives but rather suggest capabilities that the TSP must develop;
- while there is a distinction between protecting TSP networks and protecting end-users from cyber security threats, it appears throughout the CSTAC documents that protecting end-users is considered an optional feature;[13] and

[12] These reasons include (i) confirming and corroborating bot infections via multiple data points, (ii) minimizing the possibility of false positive identification of hosts, (iii) confirming the infection's intent or malicious nature, (iv) estimating the severity of threat the infection poses, (v) determining the potential methods for eventual remediation, and (vi) enabling continuous monitoring to account for the typical dynamic nature of botnets.

[13] For example, the report states that "Nothing in these policies and standards limit a CTSP's [Canadian Telecommunications Service Provider] ability to restrict which features are available at which service levels, or to charge for those features."

- the CSTAC best practices do not address certain commonly recognized approaches to preventing harmful traffic (e.g., spam transiting TSPs' networks), like blocking outbound Simple Mail Transfer Protocol traffic.

52. The Commission also reviewed other best practices referenced by parties, including BITAG's report issued in 2013, which showed that certain ports commonly run services that are vulnerable to abuse on the Internet.[14]

53. In response to the RFIs, only one TSP claimed to block certain ports for security purposes in accordance with BITAG's report. However, review of TCI's submission and of the disclosures by Bell MTS and TekSavvy, as well as the technical support forums of several other Canadian TSPs that include comments from subscribers, suggest that this practice is more frequent. Alternatively, through their acceptable usage policies, TSPs seek to limit communications on certain ports commonly associated with network abuse.

54. Finally, given the lack of basic metrics for tracking the results of the TSPs' blocking activities, the Commission is not in a position to fully assess the effectiveness of the current botnet-blocking mechanisms.

TSPs are uniquely positioned to address botnet activity

55. While the Commission recognizes that other stakeholders have a role to play in botnet mitigation, this proceeding is limited to TSPs' blocking of botnets because it is this activity that falls within the scope of the Act. The Commission considers that a requirement on TSPs engaged in botnet blocking to provide a baseline level of protection would complement, and not replace or limit, other initiatives to address botnets, such as collaboration, education, policy, and end-user notification.

56. In the same vein, the Commission considers that no single entity in the cyber security landscape, including TSPs, can resolve the botnet issue alone. Responses to botnets, given their complexity, persistence, and impact, are widely considered to require a "defense in depth"[15] approach. Under this approach, several layers of security controls are combined to protect against single points of failure.

57. To date, most of the burden to secure devices against malware threats has fallen on end-users. While it is true that end-users are in the best position to address malware infections at their source, they have a daunting list of responsibilities if they wish to

---

[14] The term "port blocking" used in BITAG's report refers to a TSP's practice of identifying Internet traffic by a particular transport protocol and port number (an integer that uniquely identifies a particular service on the endpoint of a communication stream), and blocking it entirely. Simple Mail Transfer Protocol communications over port 25 are an example of a transport protocol and port that is blocked by some TSPs to prevent network abuse, such as spam email.

[15] The Certified Information Systems Security Professional Official Study Guide states that "Defense in depth, also known as layering, is the use of multiple controls in a series. No one control can protect against all possible threats. Using a multilayered solution allows for numerous different controls to guard against whatever threats come to pass."

successfully do so. For example, they must install and update antivirus solutions, perform regular software updates, install and manage a firewall, use strong passwords, enable two-factor authentication, and secure their wireless connection, all while maintaining a persistent vigilance against online threats in an ever-evolving threat environment.

58. In reality, most end-users with a malware-infected device are unaware of the infection. Even when notified, they often lack the technical competency to remediate the issue and prevent future incidents, or do not respond to the infection because they are unaware of the risks associated with botnets. Another consideration is that many end-users own several devices and cannot bear the added cost of antivirus software or host-based firewalls on each machine in their home network. Even if this were not the case, Internet of Things devices with low computing capabilities and limited to no capacity for updates or antivirus solutions could prevent even the most diligent end-users from adopting appropriate security controls.

59. While it is true that TSPs cannot address bot infections at their source, their position as Internet access providers means they are a critical control point for botnet communications. They have a much broader view of the issue and, therefore, have more opportunities to disrupt botnet communication channels at scale. Moreover, unlike many end-users, they have the skill, expertise, and capacity to understand the botnet threat and respond proportionately.

60. Further, section 4.1 of the CSTAC best practices recognizes that there are times when a TSP can detect an infection that an end-user cannot because malware writers take steps to avoid detection by end-user security controls.

Network-level blocking is effective and appropriate

61. The Commission considers that network-level blocking should be put in place in addition to, and not in lieu of, other initiatives (e.g., consumer and stakeholder education and collaboration) to achieve the best results.

62. The Commission further considers that no single security control is 100% effective. This applies to botnets because certain techniques may evade network-level blocking (e.g., fast flux, domain generation algorithms, and peer-to-peer botnet architectures).

63. Nonetheless, the Commission considers that network-level blocking is an effective and appropriate mechanism for the following reasons:

    - Most Canadian carriers have invested resources in network-level blocking of their own initiative for many years.

- The CIRA Canadian Shield is successful. Despite its low adoption rate by the general public,[16] the solution has blocked more than 20 million malicious domain requests for its 100,000 users in its first seven months of operation. In addition, according to CIRA's website, CIRA recently entered into a partnership with Mozilla Firefox, by virtue of which the service is enabled by default for users of the web browser. Under the partnership, Canadian Mozilla Firefox users' web traffic is filtered by default by CIRA Canadian Shield blocking infrastructure. This initiative has been deployed over the course of this proceeding. It began in July 2021 and had reached 100% of Canadian Mozilla Firefox users by late September 2021. According to its website, CIRA has since blocked approximately one malicious domain per user every day.
- The federal government has implemented network-level blocking for its own network. The CSE, which is the technical authority for cyber security in Canada and the manager of the blocklist for the federal government's network, considers that a new network-level blocking framework would improve Canadians' average level of cyber security.
- Other countries have implemented such solutions.
- A narrowly constrained blocking mechanism would have a minimal, or even nonexistent, net impact on net neutrality.[17] While some might characterize botnet blocking as inconsistent with net neutrality in that it blocks the delivery of telecommunications, it also has a role in preserving net neutrality. Not only does such a mechanism serve to protect Internet accessibility, a necessary condition for net neutrality, it also corrects the distortion created by botnets in the overall Internet bandwidth resulting from the significant and unfair advantage in favour of machine-generated traffic from cyber threat actors. Accordingly, the Commission considers that the benefits of botnet blocking for Canadians and for carriers' networks outweigh the minimal, or nonexistent, net impact on net neutrality, provided that botnet blocking is subject to appropriate constraints.

There is confusion among the parties regarding the regulatory basis for the existing botnet blocking conducted by TSPs

64. In Telecom Regulatory Policy 2009-657, the Commission provided TSPs with guidance on the use of Internet Traffic Management Practices (ITMPs) to reduce or prevent congestion on their networks.

---

[16] In order to opt-in to CIRA Canadian Shield, users need to manually configure their router to send domain lookups to CIRA's resolver, which requires a measure of technical skill. Many Canadians may also be unaware that CIRA offers this service. These factors provide possible explanations for the low adoption rate.

[17] Net neutrality is the concept that all traffic on the Internet should be given equal treatment by TSPs with little to no manipulation, interference, prioritization, discrimination, or preference given.

65. Based on paragraphs 44 and 45 of Telecom Regulatory Policy 2009-657, blocking for the purpose of network security, including blocking botnet traffic, was not explicitly dealt with as part of the ITMP framework. Indeed, the principal justification for the ITMP framework was managing network congestion rather than addressing security concerns. However, the Commission noted in paragraph 44 that certain ITMPs were employed to protect users from network threats. The Commission was therefore of the view that such activities were unlikely to trigger complaints or concerns under the Act. Based on the record of the current proceeding, the Commission notes that parties have interpreted the language of paragraph 44 in a variety of ways and that there is some confusion as to the authority of TSPs to engage in botnet blocking in accordance with the Act. The Commission considers that stakeholders would benefit from additional clarity and a consistent approach to botnet blocking under the Act.

66. In accordance with section 36 of the Act, Canadian carriers must obtain the Commission's prior approval in order to control the content or influence the meaning or purpose of telecommunications they carry for the public. Blocking botnet transmission can prevent the delivery of telecommunications to the intended recipient. The ultimate purpose and effect of blocking such botnet telecommunications is to prevent the delivery of malicious content to end-users. Thus, by blocking such botnet telecommunications, a Canadian carrier exercises control over the content of those telecommunications it carries for the public, or influences their purpose. Accordingly, such activity falls within the scope of section 36 of the Act. With respect to Bell Canada's argument that carriers are permitted to block botnets under CASL, the Commission considers that its powers under section 36 are not affected by subsection 7(2) of CASL.[18] Rather, subsection 7(2) only serves to exclude certain activities conducted by TSPs from the prohibition set out in subsection 7(1) of CASL, which relates to the altering of transmission data in an electronic message.

Conclusion

67. In light of the above, the Commission finds that regulatory measures are necessary because (i) TSPs' current practices are diverse and opaque and depend on ineffective manual and ad hoc communications for sharing; (ii) TSPs have a considerable role to play in botnet blocking, consistent with a defence-in-depth strategy toward cyber security; (iii) network-level blocking programs are effective and appropriate; and (iv) there is confusion among the parties regarding the regulatory basis for the existing botnet blocking conducted by TSPs.

---

[18] Subsection 7(2) states that "subsection (1) does not apply if the alteration is made by a telecommunications service provider for the purposes of network management."

If the problem of botnet traffic necessitates regulatory action, what kind of regulatory action would be appropriate?

The Commission's position in the Notice of Consultation

68. In the Notice of Consultation, the Commission called for comments on the appropriateness and effectiveness of the regulatory mechanisms listed.

Positions of parties

69. Jonathan Curtis, Kristin Surette, CIRA, Cogeco, Eastlink, the Internet Society, Lumen Technologies Inc., the M3AAWG, Nokia, Open-Xchange AG, PIAC, SaskTel, Shaw, TekSavvy, and Vaxination Informatique argued against a one-size-fits-all solution or a mandated top-down regulatory option, which would impose a rigid technical solution for blocking botnet traffic on all TSPs. In general, this category of interventions relied heavily on continued cooperation and education. The interveners favoured the use of a voluntary code of conduct or guiding principles set by the Commission that would grant TSPs the flexibility to implement and adjust their cyber security measures as they see fit. Subject to a few exceptions, these interventions generally did not provide examples of commitments or concrete solutions that could be implemented to detect and block botnet traffic under such voluntary initiatives. For example, Eastlink suggested that the Commission encourage the development of a voluntary code of conduct for TSPs, and that Eastlink continue to work with cyber security experts and experiment with different approaches to determine which is the most effective.

70. Graeme Smith, CIBC et al., Electricity Canada, the Manitoba Coalition, and Videotron supported a mandated detailed framework, but to different extents. CIBC et al. argued that voluntary blocking is already done under paragraph 44 of Telecom Regulatory Policy 2009-657 and that carriers should already have the capability to block traffic because this capability is included in CSTAC's best practices.

71. Shaw submitted that the Commission should create a straightforward voluntary framework, including a centralized blocking organization to manage a blocklist. Shaw added that given the universal benefits associated with blocking botnets and the very low cost of participating in its proposed model, it would expect every Canadian TSP to want to take advantage of Shaw's proposed Botnet Blocking Organization blocklist to protect its customers and itself from harm.

72. Dr. Benoit Dupont prepared a study for Public Safety Canada in 2013, and submitted it as part of this proceeding. The study, *An International Comparison of Anti-Botnet Partnerships*, detailed some pros and cons of voluntary versus compulsory blocking. Dr. Benoit Dupont argued that a voluntary model affords TSPs the flexibility to adapt to technological or tactical changes by threat actors, resulting in improved performance. The contrary view point is that compulsory models provide greater implementation consistency. Dr. Benoit Dupont submitted that one drawback of voluntary programs is the lack of uniformity experienced by

end-users. Dr. Benoit Dupont added that the fact that participating TSPs retain a level of independence regarding how infections are handled makes evaluating the program as a whole more difficult. It also does not protect against problems of free-riding TSPs that choose not to share information that could benefit other TSPs in their anti-botnet efforts. Dr. Benoit Dupont argued that, despite this, the Commission should start with a voluntary-based approach.

73. Similarly, PIAC submitted that any voluntary guidelines should be reviewed subsequently to confirm their effectiveness and determine whether there is new evidence of the harm botnets pose to consumers that would justify converting the voluntary guidelines into mandatory regulatory requirements.

74. Some TSPs and other parties submitted that a mandated framework would lead to costs being transferred to consumers. Bell Canada and RCCI argued that there should be compensation for associated implementation costs. SaskTel submitted that the solution should allow for flexibility in its integration, be non-bureaucratic in operation and maintenance, and be as cost-effective as possible to avoid increased rates for the end-user. The Manitoba Coalition submitted that a mandated framework would enable the Commission to ensure that the botnet-blocking framework would be industry-funded, following the Commission for Complaints for Telecom-television Services' model.

75. Dr. Benoit Dupont submitted that there was little interest for TSPs in paying for better botnet protection because their revenue is not affected by botnet activities that target consumers, financial institutions, and online ad networks, while the technical and customer service costs associated with anti-botnet programs are high. Furthermore, there is also very little evidence that end-users would be willing to pay more for better security, since they lack detailed information about the problem.

76. Regarding the scope of potential regulatory action, a number of parties submitted arguments related to whether a mandatory framework should be extended to non-carrier TSPs or not. Carriers including Eastlink and Videotron submitted that all TSPs should share the cost and burden of a mandatory blocking program. However, PIAC submitted that a mandatory framework may unfairly place regulatory burden on smaller TSPs who may not have the resources to comply with the framework. The ITPA/CCSA also opposed the application of any new framework to smaller TSPs, because this would increase the underlying costs of the services. Competitive concerns, especially those of smaller companies, preclude rate increases to compensate for these additional costs. Thus, a new mandatory framework would have a disproportionate impact on small, rural service providers compared to the larger competitors that are able to cross-market subsidize the costs of these services from their large and dense urban operating territories.

77. Dr. Benoit Dupont submitted that the local features of the Canadian digital ecosystem also need to be taken into consideration when policy is created. More specifically, Dr. Benoit Dupont's submission pointed to a 2010 study whose authors noted that Canadian TSPs account for just 42% of unique sources of spam, a reliable

indicator for botnet infected computers. This is in contrast to other nations in the Organisation for Economic Co-operation and Development, whose TSPs account for an average of almost 80% of spam. Dr. Benoit Dupont concluded that the difference suggests that a Canadian anti-botnet partnership should not be limited to TSPs but should also include the web-hosting provider industry.

Commission's analysis and determinations

78. Having considered the submissions regarding the advantages and disadvantages of mandatory and voluntary blocking, the Commission considers that the most appropriate approach in the current circumstances is to ensure that when TSPs provide network-level botnet blocking, such blocking is subject to certain minimum standards. In the Commission's view, this approach will offer TSPs the flexibility of a voluntary approach while ensuring a baseline level of protection is provided, serving the public interest and furthering the telecommunications policy objectives set out in the Act.

79. In the following section, the Commission sets out the guiding principles to govern any botnet-blocking mechanism. Following further processes, the Commission will impose these minimum standards, including certain basic parameters, as conditions of its approval of any network-level botnet blocking, pursuant to section 36 of the Act.

80. While this framework would apply only to Canadian carriers, the Commission encourages non-carrier TSPs to adopt a similar approach. If non-carrier TSPs engage in botnet blocking in a manner that is inconsistent with the minimum standards established by the Commission, the Commission may consider whether it is necessary and appropriate to impose such standards as conditions of service pursuant to section 24.1 of the Act.

What are the technical parameters of a blocking framework?

Blocking techniques

The Commission's position in the Notice of Consultation

81. In the Notice of Consultation, the Commission invited comments on the technical aspects of a network-blocking framework, including blocking techniques, domain resolver selection, and adaptation to technological changes.

Positions of parties

82. Dr. Fenwick McKelvey and Dr. Reza Rajabiun, Marc Nanni, Bell Canada, CIBC et al., CIRA, the CSE, Eastlink, Electricity Canada, the Internet Society, the ITPA/CCSA, Lumen Technologies Inc., the M3AAWG, Nokia, PIAC, RCCI, and SaskTel submitted that the framework must be technologically neutral and provide TSPs with the flexibility to choose an appropriate network-level blocking technique in a given situation because no single technique is effective for stopping botnets. For example, CIRA and PIAC suggested that the framework set guiding principles, such

as principles related to transparency, non-discrimination, necessity, proportionality, accountability, accuracy, and privacy, rather than technical blocking standards.

83. RCCI added that should the Commission determine it necessary to mandate blocking by TSPs, the TSPs should be left to design and implement a solution of their choosing because they know the limitations of their networks. CIBC et al. agreed and suggested that the framework incorporate broad language to ensure appropriate flexibility for TSPs.

84. Other interveners submitted that the Commission's regulatory intervention could be more granular and provided comments on certain forms of blocking.

85. In summary, parties submitted that domain-based blocking provides a combination of low implementation costs and a low risk of over-blocking (Cogeco's, Nokia's, and Videotron's submissions), but that its effectiveness is limited (Jonathan Curtis', the CCCS', Cogeco's, Eastlink's, M3AAWG's, and Nokia's submissions) because many malware families do not use the Domain Name System (DNS) and, even when they do, domain-blocking is easily subverted.[19] Another blocking technique is IP-based blocking, which parties generally considered more effective even though it can still be evaded through certain techniques used by threat actors (e.g., fast flux). Bell Canada, Cogeco, Nokia, and Videotron submitted, however, that the downsides of IP-based blocking are its higher risks of over-blocking and higher maintenance costs due to the dynamic nature of IPs. Bell Canada also noted that protocol-blocking (communication protocol and/or service port) is typically performed in combination with an IP address, a method that is sometimes called network socket blocking.

Commission's analysis and determinations

86. The Commission reviewed the different blocking techniques mentioned by the parties, including blocking methods based on domain, URL [Uniform Resource Locators], IP, signature, and communication protocol and/or service port, as well as other methods. The Commission finds that each of these techniques has different advantages and drawbacks in terms of effectiveness, accuracy, implementation and maintenance costs, and network performance.

87. The Commission considers that the record does not demonstrate that any one method clearly outweighs the others, but rather suggests that these methods are complementary and that carriers may wish to implement more than one to achieve the best result in a given situation.

---

[19] Protocols like DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) encrypt DNS requests in a manner that bypasses a TSP's domain resolvers and so will bypass TSP-implemented domain blocks. In addition, botnet developers can employ domain generation algorithms to ensure bots check-in with a near infinite list of derived backup domains. Other tactics that impair domain-based blocking effectiveness include peer-to-peer architectures and implementation within non-DNS-based decentralized networks, such as Tor [The Onion Router].

88. The Commission is of the view that any framework for network-level botnet blocking must be technologically neutral and must not be limited to a particular type of blocking. This will allow TSPs to adapt to technological changes and techniques employed by botmasters since the nature of the threats posed by botnets is such that they will continually outpace any attempt to prescriptively regulate solutions.

Centralized versus decentralized management

The Commission's position in the Notice of Consultation

89. The Commission sought guidance on which parties are best suited to decide what is blocked. Decisions to block should not be made lightly and must take into account factors such as the level of potential harm to Internet users and whether the blocking will have other unintended effects.

90. In the Notice of Consultation, the Commission set out its preliminary view that an independent party with expertise in cyber security would be best suited to assess the impact of blocking a particular domain or IP address with a view to protecting the public interest, and to decide whether blocking is warranted. The Commission also stated its view that carriers and TSPs should be required to seek approval from the independent assessor before adding new blocklist indicators, but recognized that TSPs may require the flexibility to remove indicators that lead to false positives from the blocklist in order to protect the integrity of the framework.

Positions of parties

91. Bell Canada, Eastlink, RCCI, SaskTel, and TCI submitted that it should be left up to individual TSPs to design and implement the solution that is best suited to their respective existing network capabilities. The M3AAWG was also supportive of a decentralized provider-by-provider filtering regime, on a voluntary basis, over the adoption of a single independent party to make industry-wide blocking or filtering decisions. CIRA submitted that it is key that any framework avoid a single point of failure. Regarding the implementation of a decentralized model, CIRA suggested that blocklist providers would have to comply with certain service standards and requirements (e.g., standards for timeliness to ensure fundamental redress) to be accredited.

92. Shaw was in favour of a centralized botnet blocklist that would be used by all Canadian TSPs. The Commission's role would be limited to setting blocking principles and designating a botnet-blocking organization that would manage the blocklist and the appeal mechanism in case of false positives. Cogeco and Videotron also supported a focused type of blocking (domain-based), through which an independent third party with expertise in cyber security would be charged with providing all TSPs with a blocklist. Videotron submitted that an independent blocking organization would reinforce the legitimacy of the blocking framework for consumers. It added that a flexible system, where each TSP could choose their own blocking method, as supported by Bell Canada, RCCI, and TCI, would lead to inconsistencies and confusion for consumers. While PIAC did not specify whether it

would prefer a centrally-managed blocklist, it submitted that the Commission should encourage TSPs to share intelligence about botnet activity on their networks to foster a more coordinated response to network security.

93. A majority of parties, regardless of whether they were opposed to a framework in general or in favour of a mandated or voluntary model, preferred involving an independent party with experience in cyber security instead of having an entirely decentralized approach. For example, Vaxination Informatique stated that this system should in no way be left to any one TSP or TSP association. Open-Xchange AG echoed this position and submitted that the Commission should ensure that the appropriate balance between security and data protection needs is not left up to individual operators.

94. The following third parties with expertise in cyber security were suggested as independent parties that could be involved in developing a blocking mechanism:

    - the Canadian Coalition Against Internet Child Exploitation;
    - the Canadian Cyber Threat Exchange (CCTX);[20]
    - the CCCS;
    - CIRA;
    - the Commission;
    - CSTAC; and
    - a newly created independent organization.

95. Dr. Benoit Dupont submitted that the Commission could be a good candidate to overview the blocking framework, given its long experience as a telecommunications regulator, and suggested that a framework would be more legitimate if it were supervised by the Commission. Vaxination Informatique proposed an informal system to reduce overhead costs but still provide oversight, where a central body such as the CCCS or the CSE would validate threats, and the Commission would disseminate these threat reports to all TSPs with the authority to block the threats. The Commission would also set an expiry date for the threats so that the blocks are temporary. TSPs would then be free to implement or ignore a threat report.

96. Some parties submitted that asking for permission to block threats would be counterproductive because many TSPs are already routinely blocking malicious traffic, and the damage from the threats would already have been done.

---

[20] The CCTX is Canada's cyber threat collaboration forum and source of cyber threat intelligence, where private and public organizations collaborate to reduce cyber security risks. The CCTX runs both the CCTX Data Exchange and the CCTX Collaboration Centre. The CCTX Data Exchange is where CCTX gathers, analyzes, and shares cyber threat intelligence across business, government, and international threat-sharing hubs.

97. The CSE submitted that it can provide an IOC feed to the Commission and any interested parties but did not commit to managing a blocklist for TSPs. The CSE added that because it is not a regulator, it should not have decision-making authority in any proposed framework. The CSE further submitted that it is not the only source of high-confidence IOCs and suggested that the Commission consider other threat intelligence feeds. The CSE concluded that CIRA Canadian Shield could also be used.

98. Vaxination Informatique expressed its concern with certain third parties being given discretion to block threats and submitted that the Commission should provide a level of accountability through public disclosure.

99. The M3AAWG argued that permitting TSPs to use third-party blocklists in their implementation of the blocking framework, as an alternative to centralized blocking decisions, is not without its drawbacks. The M3AAWG submitted that when it comes to data from third-party sources, like domain name server blocklists, the data is typically offered on a take-it-or-leave-it basis. Where third party blocklist providers defer risk associated with the use of their blocklist to the blocklist user, the M3AAWG added that TSPs and mobile carriers can mitigate those risks by defining and implementing criteria for the selection of the domain blocklist providers they use. An example is the criteria defined by the Internet Corporation for Assigned Names and Numbers in the methodology of its Domain Abuse Activity Reporting System.

Commission's analysis and determinations

100. The Commission considered (i) the general benefits and drawbacks of having some form of centralization, and (ii) the potential candidates proposed by the interveners that could serve as the central authority of a blocking framework, including their expertise and independence, as well as the ease of implementation.

General benefits and drawbacks of having some form of centralization

101. The sharing of IOCs among TSPs currently depends on ad hoc communications. The Commission recognizes that there may be commercial limitations on a TSP's ability to share information from a commercially-provided third-party blocklist. The Commission considers that a certain level of centralization would address this gap by ensuring that all TSPs have a baseline level of information, which would in turn ensure a baseline level of protection for all customers. The Commission considers that having a centrally-managed blocklist would necessarily increase the visibility of false positives and decrease the risk of over-blocking.

102. The Commission is therefore of the view that a centralized blocklist is the most efficient and effective option. Nevertheless, a minimum framework for network-level botnet blocking must allow for TSPs to implement complementary initiatives. Such initiatives, for example, may include proprietary systems and third parties' blocklists to protect their networks and customers from cyber threats.

103. The Commission acknowledges that having a variety of blocklists or systems is generally less transparent to the public and makes obtaining compiled metrics more complex (e.g., what is blocked by which system). However, and more importantly, having a variety of solutions makes it more difficult for botnet operators to gain widespread entry into the networks and the customers' systems. The Commission also considers that enhancements to a baseline blocklist with other proprietary or third-party systems could foster innovation and competition among TSPs and third parties. However, the use of additional blocklists raises the issue of whether they would be assessed and accredited, and if so, how and by whom.

104. The Commission considers that there are several benefits to accrediting additional blocklists. Accreditation would ensure that TSPs implement network-level botnet blocking in compliance with the minimum framework established by the Commission. It would also ensure that blocklist providers have sufficient technical expertise.

Potential candidates proposed by interveners that could serve as the central authority of a blocking framework

105. The CCCS is Canada's technical authority on cyber security. The CCCS brings together existing operational cyber security expertise from the CSE, Public Safety Canada, and Shared Services Canada into a single organization. In addition to its expertise in cyber security and its neutrality, the CCCS also has the benefit of being a CSTAC member and is already working collaboratively with TSPs and the RCMP. In addition, it already manages a blocklist for the Government of Canada and provides a data feed to the CCTX.

106. With regard to the CCTX and CSTAC, there is no doubt that both organizations have the necessary expertise in cyber security. However, since Bell Canada is a CCTX founder and the current CCTX Board Chair, and since RCCI is CSTAC's Industry Co-Chair, some stakeholders may not regard these organizations as neutral third parties. In addition, CCTX membership costs range from $500 to $50,000. CSTAC membership is limited to 12 TSPs and thus does not represent the interests of all TSPs. These factors further limit the appropriateness of these organizations serving as blocklist managers.

107. Another option, as suggested by the CCCS, is to leverage CIRA Canadian Shield. CIRA has the expertise and is relatively independent from TSPs.[21] As previously stated, CIRA blocked 20 million domains over 12 months, and 50,000 of these are based on the CCCS blocklist. This means that CIRA's blocklist is much more extensive than the one created by the CCCS. However, CIRA mentions that it currently serves more than 500 million queries each day through CIRA Canadian Shield. This means that using CIRA Canadian Shield would only be feasible if CIRA were able to scale its systems to handle much more traffic. If CIRA is unable

[21] CIRA is a private, not-for-profit organization. A few board members at CIRA also hold executive positions in the TSP community.

to scale its systems to the extent required, this option will not be feasible. Other issues that may arise in using CIRA's DNS infrastructure rather than that of carriers include the risk of a single point of failure, complications for customer support, and the increase in average DNS response latency.

108. The Commission also rejects the suggestion in favour of its own involvement, given its current lack of expertise and resources to support the management, curation, and/or distribution of a centralized network blocklist. Further, the Commission does not consider that it should be involved in the handling of false positive complaints, which require resolution in a matter of hours.

109. The last option is to create a new standalone organization. This would take time and be costly. Further, in the Commission's view, it could be unduly burdensome.

110. In light of the above, the Commission considers that there is currently no single organization ready to manage a centralized blocklist for use by Canadian TSPs. However, as noted above, complete centralization is not necessarily required.

111. The Commission therefore requests that the CRTC Interconnection Steering Committee (CISC) examine whether an independent organization (such as the CCCS or CIRA) is able and willing to maintain a baseline blocklist for use by TSPs in Canada. The Commission requests that CISC also examine whether and how complementary or alternative systems (i.e., third parties' blocklists, proprietary systems, and practices such as standard service port blocking or other recommended best practices) may be accredited or subject to technical requirements. Such systems could be used to complement a centralized blocklist, or in place of a centralized blocklist if that is not a viable option. Detailed questions for CISC are in Appendix 2 to this decision.

112. The Commission requests that CISC file a report within **nine months** of the date of this decision. Interested parties will have an opportunity to comment on the report prior to the Commission rendering any further determinations regarding the framework to be applied to network-level botnet blocking.

113. Although the Commission is referring these matters to CISC, it notes the existence of working groups such as CSTAC, where stakeholders can have more in-depth and private deliberations on sensitive security issues, if necessary.

Block-by-default, opt-in, and opt-out models

The Commission's position in the Notice of Consultation

114. In the Notice of Consultation, the Commission stated that infected Internet-connected devices operating as bots generally do so without the owner's knowledge or consent. The Commission also recognized that Internet service subscribers may not see the benefit of participating in a network-level botnet-blocking program, even if their device is infected with malware. Considering these factors, the Commission indicated its preliminary preference for a block-by-default model but invited parties

to compare and contrast the effectiveness of block-by-default, opt-in, and opt-out models to address botnet communications.

Positions of parties

115. Several parties, particularly TSPs, favoured a block-by-default model rather than opt-in or opt-out approaches.

116. Eastlink, RCCI, SaskTel, and Shaw, for example, endorsed a block-by-default model and took the position that there should be no opt-in or opt-out process because network protection is beneficial and applicable to everybody. They submitted that opt-in and opt-out models both place increased administrative burden on TSPs. Shaw used Cleanfeed[22] as an example of a block-by-default model it considers to be useful and applicable to blocking botnets.

117. Bell Canada was also in favour of a block-by-default model and argued that it currently lacks the capability to implement an opt-in or opt-out model as part of botnet blocking. Bell Canada explained that network-level blocking, where the blocking functionality is always on, does not distinguish between each Internet user. Instead, it is typically uniformly applied across the TSP's networks without being customizable by individual users. Bell Canada submitted that the advantage of the always-on blocking functionality is that it provides protection from botnets while avoiding the added costs of having to build new dynamic IP address-tracking mechanisms linked to customer account information (costs that would inevitably be passed on to Internet customers). Bell Canada also claimed that the block-by-default model avoids the increased collection and use of customers' personal information.

118. Nokia, from the perspective of a threat intelligence provider, supported the TSPs' argument that opt-in and opt-out may be impractical for them to implement and manage. Nokia submitted that if the technology is accurate and reliable, it could be possible to use the block-by-default model and provide an opt-out functionality. It added that the flexibility afforded through the opt-in or opt-out models increases costs to carriers and, ultimately, to users.

119. CIBC et al. submitted that opting out from being protected not only impacts the user who opts out, but also other users within the TSP network. Allowing users who have opted out to remain inside a TSP's trusted network of botnet-protected devices would have tangible negative impacts. CIBC et al. concluded by recommending the block-by-default approach.

120. J. Clarke, Dr. Fenwick McKelvey and Dr. Reza Rajabiun, the Internet Society, TCI, and TekSavvy argued in favour of an opt-in model, but offered different rationales for their support of it.

---

[22] Under project Cleanfeed, Canada's largest TSPs, including Bell Canada, MTS Allstream, RCCI, Shaw, SaskTel, TCI, and Videotron, have blocked access to websites displaying child exploitation material since 2006 and 2007.

121. J. Clarke and TCI submitted that the private sector already offers blocking services that customers can opt into, and that these service providers have the necessary resources to generate and maintain blocklists. The Internet Society, in its support for an opt-in model, recommended that prospective users be made aware of the potential implications of opting in and of consent to participation on a periodic basis. Dr. Fenwick McKelvey and Dr. Reza Rajabiun submitted that blocking Internet resources outside a TSP's network should only be addressed via an opt-in model, and that if TSPs want to offer additional protections to their customers, they should do so on an opt-in basis as part of a bundled package made available free of charge.

122. Parties in favour of an opt-out model were predominantly not-for-profit organizations or individuals. Open-Xchange AG considered that blocking content that potentially causes damage is a collective good and recommended blocking be turned on by default. However, it suggested that an opt-out mechanism be made available for certain individuals, such as malware researchers. The M3AAWG was in favour of an opt-out model because opt-in may have low uptake. CIRA favoured an opt-out model because it considered it important that subscribers be able to exercise their right to choose. Focus group participants in the survey led by the Manitoba Coalition preferred an opt-out model through which customers would receive notifications of blocking events and could report false positives. Kristin Surette considered the opt-out method appropriate because botnets typically operate from personal computers, without the owners' knowledge.

Commission's analysis and determinations

123. The Commission notes the historically low uptake of opt-in approaches. Despite providing a free service available to all Canadians, CIRA Canadian Shield is used by just 1% of households. This very low figure suggests that opt-in models result in underuse. The Commission considers, however, that the fact that users may not take positive steps to opt-in to a botnet-blocking service does not mean they would prefer that their devices and networks be exposed to a malicious botnet.

124. While an opt-out model does not present the issue of underuse, the Commission considers there are other disadvantages to that model. Both opt-in and opt-out models undermine security, especially that of other users. Since network protection is beneficial to all users, it should apply to everybody.

125. The Commission also considers that opt-in and opt-out models significantly increase the implementation burden and costs borne by TSPs, can delay the implementation of the blocking mechanism, and can be overly burdensome to manage.

126. The Commission finds that neither opt-in nor opt-out options are appropriate and that, where network-level blocking is provided, it should apply by default. This approach would ensure that all the TSP's customers benefit from the blocking in the most efficient and effective manner. The Commission notes that the blocking-by-default model is consistent with the Cleanfeed blocking model and with CIRA's current blocking model resulting from its partnership with Mozilla Firefox.

127. The Commission notes that the framework would not be totally deprived of opt-out mechanisms because users and researchers may (i) use VPN [virtual private network] services to which the blocking would not apply, (ii) use information about TSP blocking practices to inform their choice of service provider, or (iii) direct domain requests to resolvers that circumvent the blocking conducted by certain TSPs.

Technical scope (types of IOCs)

Positions of parties

128. Some parties supported a broader framework on cyber security, whether or not it was related to botnets. For example, the Digital ID & Authentication Council of Canada submitted that strengthening a cyber security framework that addresses more diverse cyber security threats and takes a more holistic look at Internet security would better serve the Commission, Canadians, and Canadian businesses.

129. Similarly, the CSE submitted that, based on its experience defending the networks of the Government of Canada, it believes that the "botnet" wording is too narrow in scope. The CSE added that it recommends expanding the scope to allow blocking general IOCs, much in the way that it blocks such IOCs for the Government of Canada.

130. By contrast, Samuel Harper, CIRA, INFOSECSW, the Internet Society, and Vaxination Informatique expressed significant concerns that a new framework may be a slippery slope toward content blocking and citizen surveillance. For example, CIRA submitted that it was deeply concerned that any such voluntary framework could be hijacked for purposes that stray from network integrity and security in any manner. It argued that the end result of this proceeding, or of the Commission's activities in this area, must not be the development of a more accessible master switch that nudges common carriers toward a role as editors, filters, or sheriffs of the Internet. Vaxination Informatique similarly submitted that this project must be extremely well circumscribed, with a very specific and narrow mandate that does not allow for any gradual broadening.

Commission's analysis and determinations

131. The Commission notes that botnets, malware, and computer intrusions are intertwined, making it impractical and inefficient to block only botnet traffic and not block other types of IOCs. In fact, TSPs currently filter IOCs based on blocklists regardless of their source (botnets or not). Moreover, the policy justification for blocking botnet traffic (i.e., the harm caused to Canadians by cyber threats) applies equally to other IOCs. Accordingly, as a matter of policy, the CSE's recommendation for an approach that focuses on all IOCs rather than on botnet traffic, which in practice is not isolated to a specific IOC, may be appropriate. An approach centred on IOCs would have to be extremely well circumscribed to ensure it is limited to cyber security and precludes any gradual broadening of its scope.

132. Further, the Commission considers on a preliminary basis that the blocking of other IOCs should be subject to the same guiding principles as the blocking of botnet traffic. The Commission requests that CISC confirm certain technical considerations related to IOCs as detailed in Appendix 2 to this decision. The Commission will publish the CISC report on its website, where interested persons will have an opportunity to comment.

Safeguards regarding privacy

The Commission's position in the Notice of Consultation

133. In the Notice of Consultation, the Commission stated that botnets pose a significant threat to consumer privacy when they access personal information, and that blocking botnet communications can help protect consumers. However, this protection is achieved by monitoring Internet traffic. The consequences for consumer privacy caused by monitoring are important issues for any potential blocking framework to address. The Commission invited parties to comment on conditions that can protect consumer privacy.

Positions of parties

134. Videotron submitted that the conditions for protecting consumers' privacy are already laid out in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the related jurisprudence. In this context, exceptions apply for accessing personal information for law enforcement purposes.

135. Bell Canada and SaskTel argued that, based on their experience, network-level blocking does not raise privacy concerns because it does not rely on content-based indicators or reveal identifiable customer-specific information.

136. As outlined below, a number of parties expressed the view that specific safeguards should be set regarding how personal information is collected, used, retained, and disclosed. More specifically, CIRA submitted that the Commission should establish a higher standard of privacy protection than what would be available under PIPEDA, as acknowledged by the Commission through Telecom Decision 86-7 and other related decisions regarding telephone services' consumer confidentiality safeguards.

137. The Manitoba Coalition submitted that privacy is a priority for consumers. It suggested that an independent decision-making body should be created and strict restrictions imposed on what information is collected and monitored and what is ultimately done with that information. Dr. Benoit Dupont also noted that privacy and accountability should be held at the highest standard in order to avoid controversy and gradual broadening of surveillance.

138. Dr. Fenwick McKelvey and Dr. Reza Rajabiun submitted that all the types of information collected for the purpose of combatting botnets should be included in the Commission's determination, and that the data collected cannot be sold to third parties.

139. Shaw argued that blocked information should be limited, and that the blocking mechanism should follow these principles:

- Limited purpose for collection, use, and retention: TSPs and the blocking organization should only collect, use, disclose, and retain data necessary to block botnets.
- Transparency: TSPs' privacy policies should clearly state that limited information will be collected and used to block botnets.
- Defined process: TSPs should have a process to document data collected and processed in the course of managing their botnet-blocking system.
- Appropriate mechanism for data deletion: TSPs should have a process to effectively manage and dispose of the data collected through this data processing, including keeping it separate from other data.

140. Open-Xchange AG also mentioned that any personal information collected must not be used for other purposes. Blocked destinations should be collected for the purpose of end-user notification of infection but subject to a time limit (e.g., 30 days), after which the data collected is destroyed. CIPPIC submitted that rules regarding proper deletion need to be included in any type of framework for carriers.

Commission's analysis and determinations

141. The Commission acknowledges the view of some TSPs that network-level botnet blocking does not generally reveal identifiable customer-specific information. Nevertheless, the Commission considers that where personal customer information is collected, used, or disclosed, safeguards for the protection of that information are of critical importance. TSPs are already required to comply with existing legal obligations regarding the collection, use, and disclosure of personal customer information.[23] In addition, the Commission would expect TSPs to implement best practices that enhance such obligations to account for the specifics of a blocking framework and ensure that confidential customer information collected, used, or disclosed for the purpose of the blocking mechanism is limited to that which is essential for that purpose, and only for so long as it is necessary for that purpose, and that the information collected is not used or disclosed for any other purpose. The corresponding principle is set out in Appendix 1 to this decision.

142. The Commission notes that CIRA conducted an audit of its processes with respect to privacy in the context of CIRA Canadian Shield. While at this stage the Commission does not consider an audit requirement to be necessary, the CIRA

[23] In addition to PIPEDA, TSPs are required to comply with consumer confidentiality safeguards imposed by the Commission, which prohibit TSPs from disclosing customer information other than name, address, and listed telephone number to any person without the customer's express consent except in certain specified circumstances (see for example Telecom Decisions 2003-33 and 2005-14 and Telecom Regulatory Policies 2009-723 and 2017-11).

report contains useful information about operational privacy safeguards to account for the specifics of a cyber security blocking solution.

Transparency and TSPs' disclosure requirements

The Commission's position in the Notice of Consultation

143. In the Notice of Consultation, the Commission asked parties to comment on the necessary disclosure requirements for TSPs. In particular, the Commission invited comments on provisions that will provide transparency about blocking programs, for example, notifying customers of the scope of the filtering mechanism or creating a subscriber portal to check whether a particular domain is being blocked.

Positions of parties

144. In general, the parties submitted that any blocking framework should be transparent to users so that they are able to provide informed consent. Publicly available information should at least explain to customers how the blocking works, who is involved, and what information is retained. In addition, SaskTel, Shaw, and Vaxination Informatique suggested that this publicly available information should provide a link to a website that lists whom to contact for more information or consists of a more detailed page hosted by the Commission or by the blocking organization. Bell Canada, RCCI, and SaskTel submitted that, for security reasons, providing generic information to users is preferred over providing detailed information.

145. CIRA submitted that it is essential that TSPs have, and that end-users continue to have, the ability to select between the cyber security providers of their choice. CIRA argued that disclosure in relation to personal information processing, such as the extent of collection and duration of retention, should be required. CIRA also suggested that the Commission set standards on how subscribers are notified when their TSP detects that a subscriber's device is infected with malware.

146. The Manitoba Coalition submitted that consumers must be well informed about the functioning and impacts of the blocking framework, including having access to transparent information about its costs.

147. CIBC et al. recommended that TSPs disclose a wide variety of information, including, but not limited to, the overall purpose of their blocking program; how traffic is being monitored, used, and disclosed; safeguards to ensure data is not misused; and the effectiveness of their program (via blocking event and false positive counts, among others).

148. Dr. Benoit Dupont submitted that the fact that participating TSPs retain a level of independence regarding how infections are handled makes evaluating the program as a whole more difficult and, unless a public disclosure approach is adopted, data on individual TSP performance is unlikely to receive public scrutiny. Dr. Benoit Dupont added that the rationale of public disclosure initiatives is to influence

underperforming TSPs by increasing the amount of blocking-related information available to the public.

149. Xplornet submitted that subscribers must be informed that participating in a network-level blocking framework cannot serve as a substitute for the maintenance of up-to-date security software on their devices.

Commission's analysis and determinations

150. The Commission considers that consumers should be adequately informed of the nature and scope of a TSP's blocking program to allow them to make informed decisions as to their choice of services and service providers.

151. The Commission considers that transparency is a key principle of a network-level blocking framework, and may be achieved through complementary measures imposed on TSPs, as detailed in Appendix 1 to this decision. These measures include

- providing information to the public regarding the general nature and scope of a TSP's blocking program; and
- reporting specific information and performance metrics to the Commission so that it can publish information such as aggregated statistics or analyze these metrics to determine whether further regulatory action is required (the format and the frequency remain to be determined).[24]

152. Specific reporting requirements will be determined following receipt of the CISC report. For example, such reporting requirements may include, for each blocklist utilized over a reporting period, disclosing the total number of unique IOCs on a blocklist, the total number of unique IOCs effectively blocked, the total number of false positive complaints reported, the total number of IOCs shared with stakeholders, and the total number of Internet subscribers involved in the blocking.

Accuracy and safeguards regarding over-blocking and false positives

The Commission's position in the Notice of Consultation

153. In the Notice of Consultation, the Commission stated that multiple online services can be provided at the same IP address, and that botnet command and control servers do not usually remain on the same device for extended periods of time. Blocking an IP address may therefore inadvertently prevent access to legitimate services, and blocking a command and control server will only be effective for a limited time. Consequently, the blocklist must be regularly updated to remain accurate, which introduces risks of over-blocking and false positives.

---

[24] For purposes of efficiency, the reporting requirements of the specific information and performance metrics might be combined with the Commission's existing requirements related to Internet traffic management purposes disclosure.

154. The Commission invited comments on blocking framework provisions or conditions that could prevent over-blocking and false positives, or that could mitigate the associated risks. Parties were asked to

- comment on the likelihood and impact of over-blocking and false positives in the context of safeguards against botnet traffic;
- set out expectations for resolving false positives and provisions to ensure timeliness and procedural fairness in the resolution process; and
- suggest options for automated means to resolve incorrectly blocked services, and their associated benefits and drawbacks.

Positions of parties

Likelihood and impact of over-blocking and false positives in the context of safeguards against botnet traffic

155. Parties largely agreed that over-blocking and false positives are inevitable but were divided on their likelihood or prevalence. The range of opinions varied from the risk being high (the M3AAWG or Xplornet, when blocking is only done via domain names and IP addresses) or significant (Eastlink and the Internet Society) to not likely (Shaw), low (Videotron, regarding domain-based blocking specifically), or inconclusive (PIAC).

156. Cogeco and Videotron argued in favour of domain-based blocking and considered it to have a lower risk of false positives than IP-based blocking. Videotron stated that it is currently implementing domain-based blocking and that, based on its experience, the risk of false positives is low.

157. Parties also recognized that systems with low over-blocking and false positive risks are less effective.

158. The CCCS submitted that the current blocklist it provides to CIRA Canadian Shield is made of high-confidence IOCs.

Expectations for resolving false positives and provisions to ensure timeliness and procedural fairness in the resolution process

159. The Manitoba Coalition suggested that, before adding an IOC to a blocklist, the organization in charge of managing the blocklist should apply blocking criteria in a manner that is evidence-based, flexible, free from commercial or political bias, and responsive to feedback received from Internet users. Eastlink also submitted that it is critical that the entity managing a blocklist has the necessary procedures in place to ensure that domains and addresses are not added to the list without sufficient evidence demonstrating the necessity and appropriateness of blocking them. Bell Canada suggested an independent verification of any referrals generated by third parties, including those from cyber security working groups, should be conducted. Bell Canada added that the entity managing the blocklist should be highly confident

that a source is malicious before blocking it. Electricity Canada added that blocking needs to be specific and targeted, and use multiple intelligence sources.

160. The CCCS submitted that, in its experience protecting the Government of Canada's networks, it established a vetting process for IOCs before blocking them to ensure minimal over-blocking and false positives.

161. Rather than vetting the IOCs, CIRA suggested that an independent party only be accountable for accrediting blocklist providers. These blocklist providers would have to comply with service standards in order to be accredited. These service standards include requirements to respond to urgent update requests from TSPs, move quickly in case of emergencies, and comply with standards for timeliness to ensure fundamental redress.

Automated means to resolve incorrectly blocked services, and their associated benefits and drawbacks

162. Nokia submitted that it is easy to add entries to these blocklists but difficult to decide when it is appropriate to remove an entry. Dr. Benoit Dupont as well as Dr. Fenwick McKelvey and Dr. Reza Rajabiun argued that blocking should only be transitory, suggesting that each blocklist IOC be assigned an expiry date.

163. Eastlink submitted that the entity managing a blocklist should quickly and accurately determine which domains and addresses should be removed from the list based on the entity's own routine monitoring and reported false positives.

164. Regarding the reception of false positive reports, most parties suggested that a process should be in place to receive them and address the issue in a timely fashion by updating the blocklist and removing any confirmed false positive. Electricity Canada stated that developing a portal for user feedback on perceived false positives could be helpful. According to CIBC et al., false positives could be reported centrally or to individual TSPs. Once reported, the report recipient would be responsible for validating the report, including ensuring it is not an attempt to unblock a malicious indicator, and validating that the existing blocking method remains appropriate.

165. However, there was no agreement among the parties on who would be in charge of updating the blocklist (including managing updates resulting from false positive claims).

166. Cogeco, the Manitoba Coalition, and Xplornet were of the view that management of the blocklist, including updating it, should be led by an independent party with expertise in cyber security and not by TSPs. According to Videotron, having the blocking centralized under an expert organization would enable a global and consistent approach, and limit the risk of false positives. Videotron also suggested implementing a communication channel to be used by TSPs for reporting false positives to the blocking organization, which would then be able to assess and address them in a timely manner. RCCI also submitted that updating the list should

not be the responsibility of TSPs, but rather the responsibility of the appropriate government body managing the list. It added that TSPs would have no insight into what is on the list. Marc Nanni and RCCI added that TSPs would not be able to handle an increase in customer complaints to call centres and cannot be responsible for offering support to customers in relation to false positive claims. Electricity Canada suggested that the Commission may wish to leverage the expertise of the CCCS.

167. SaskTel suggested that false positive claims be handled by TSPs. TCI also considered that TSPs have been effective in preventing and mitigating the risks associated with over-blocking and false positives in their current blocking practices. TCI added that TSPs' need for operational flexibility and an ability to adapt according to the nature and scope of the particular botnet threat means they cannot implement uniform provisions to reduce over-blocking and false positive risks beyond what is already set out in CSTAC's Security Best Practice Policy for Canadian Telecommunications Service Providers (TSPs).

168. The CCCS assumed that false positives would be managed by TSPs. The CCCS recommended that the Commission look at section 1.3 of CSTAC's Securing Incident Response Standard for Canadian Telecommunications Service Providers (CTSPs), given that it includes a practice related to ensuring that blocking activities have minimal likelihood of impacting legitimate traffic.

169. The M3AAWG opposed ad hoc complaint response methods by submitting that the possible rapid rate of indicator generation, which can exceed rates of 500 new indicators per minute, means that false positive and over-blocking assessors can be easily overwhelmed with complaints. It argued that the industry needs filtering implementations that work on an industrial scale.

170. SaskTel submitted that when dealing with false positives, TSPs need to act quickly to determine whether the traffic should be blocked or not and, if necessary, remedy the situation. This would not be effective if there were an approval-granting process involved.

Making a final decision regarding false positives and general oversight

171. A number of parties agreed that an escalation or appeal process should be available when the blocking is maintained. For example, Nokia submitted that establishing a mechanism to solve disputes about whether a specific site should be blocked could mitigate over-blocking. Dr. Fenwick McKelvey and Dr. Reza Rajabiun argued that judicial oversight is critical. Vaxination Informatique suggested that escalating a complaint to the Commission should be possible.

172. The CCCS submitted that the framework should incorporate an element of standard decision-making around blocking decisions, but recommended that the CCCS itself not have this decision-making authority.

173. CIPPIC submitted that any framework must include active oversight from the Commission, including spot audits of blocking mechanisms to ensure appropriate services are not blocked. CIPPIC added that when traffic management goes awry, proof is difficult to gather for end-users. It specifically referred to Compliance and Enforcement staff letters to RCCI after comprehensive tests of RCCI's throttling measures demonstrated alleged violations of the ITMP framework.

Commission's analysis and determinations

174. The Commission recognizes that over-blocking and false positives are an inevitable element of network-level blocking. Malicious services can be embedded or provided alongside legitimate services, or analyses can misinterpret artifacts or network traffic as malicious in nature when they are benign.

175. As mentioned above, carriers should not be limited to a particular type of blocking technique. In the choice of their blocking technique(s), however, carriers must ensure that any impact on legitimate services is minimized and limited to that which is necessary to achieve the objective of blocking malicious traffic.

176. Regardless of the model and blocklist used, the Commission considers that safeguards must be in place to mitigate the risk of false positives and over-blocking, including mechanisms to

- vet IOCs prior to their inclusion on any list;
- receive and investigate false positive complaints from the public;
- update the blocklist following a complaint in a timely manner;
- update the blocklist regularly, and not just following a complaint (a mix of manual review and automated IOC delisting may be appropriate[25] and blocking on a temporary basis by applying an expiry date to the presence of an IOC on a blocklist would further help to reduce false positives); and
- ensure that TSPs log their effective blocking of IOCs and periodically verify that their blocking systems work as intended.

177. The coordination between the blocklist manager and TSPs as well as their respective responsibilities for each of the steps listed above remain to be determined for each model (centralized and decentralized). The Commission notes that TSPs should have the capability to minimize and handle false positives related to blocking mechanisms in accordance with section 1.3[26] of CSTAC's Securing Incident

---

[25] Manual delisting occurs when a technically knowledgeable and trusted person reviews false positive claims to assess whether a block should be removed. Automatic delisting occurs when false positive claims are trusted but the block is automatically reinstated if it is later reaffirmed as malicious. An example of a blocklist that uses automated delisting is the Composite Block List maintained by Spamhaus.

[26] This section states that TSPs "should have the capability to […] implement strategies which will permit traffic throttling, filtering or blocking to be effective against problem traffic while minimizing the likelihood of impact on legitimate traffic."

Response Standard for Canadian Telecommunications Service Providers (CTSPs), but that this standard does not include how this capability is operationalized by TSPs.

178. A centralized blocklist would have the advantage of reducing the risk of over-blocking and false positives. In addition to having a central blocklist manager chosen for its expertise in vetting IOCs, a centralized list would be subject to broader scrutiny by TSPs and other stakeholders than any blocklist used by a TSP in isolation. It would also allow for the consolidation of false positive assessments to better ensure false positive reports are addressed in a timely and efficient manner. CIRA Canadian Shield uses a blocklist comprising vetted high confidence IOCs provided by the CCCS and, as stated on the CIRA Canadian Shield webpage, its false positive to valid block ratio is very close to zero.

179. A decentralized model does not present the same benefits. A majority of the TSPs that have already been implementing commercial blocklists did not provide information on their false positive rates, nor did they specify if they monitor that risk. The Commission considers that, in a decentralized model, additional safeguards must be in place (e.g., regarding how commercial blocklist providers are accredited and by whom), so that TSPs ensure that the third parties managing the blocklists mitigate the risk of false positives. Specific questions on this topic are addressed to CISC in Appendix 2 to this decision.

Conclusion

180. The Commission concludes that botnet traffic constitutes a significant issue for cyber security, both in terms of volume and severity of harm.

181. The Commission finds that regulatory measures are necessary because (i) TSPs' current practices are diverse and opaque and lack a practical and consistent mechanism for sharing botnet IOCs; (ii) TSPs have a considerable role to play in botnet blocking, consistent with a defence-in-depth strategy toward cyber security; (iii) network-level blocking programs are effective and appropriate; and (iv) there is confusion among the parties regarding the regulatory basis for the existing botnet blocking conducted by TSPs.

182. The Commission finds that regulatory measures are required to ensure that the network-level botnet blocking provided by Canadian carriers provides a baseline level of protection. In summary, where network-level blocking is provided, it must comply with the following guiding principles: (i) necessity, (ii) customer privacy, (iii) accountability, (iv) transparency, and (v) accuracy. These principles, described in Appendix 1 to this decision, are intended to be technology-neutral to allow flexibility in blocking tools and techniques so that carriers can rapidly adapt to the associated sophisticated cyber threats as they evolve.

183. The Commission requests that the CISC Network Working Group propose the basic technical parameters of the blocking mechanism that could be used, in compliance with the principles set out in Appendix 1 to this decision, and file a report with the Commission. The basic technical parameters for the blocking mechanism must

include, at a minimum, (i) who will determine what is blocked, (ii) what precisely is blocked, and (iii) other technical details related to the implementation of the blocking mechanism, as outlined in Appendix 2 to this decision.

The Commission requests that CISC file a report within **nine months** of the date of this decision, addressing the matters set out above. Interested parties will have an opportunity to comment on the report prior to the Commission rendering any further determinations regarding the minimum standards that will form part of the framework to be applied to network-level botnet blocking.

Policy Directions

184. The 2006 Policy Direction[27] and the 2019 Policy Direction[28] state that the Commission, in exercising its powers and performing its duties under the Act, shall implement the policy objectives set out in section 7 of the Act in accordance with the considerations set out therein, and should specify how its decisions can, as applicable, promote competition, affordability, consumer interests, and innovation.

185. Network-level blocking of botnet traffic that complies with the guiding principles set out in Appendix 1 to this decision will help to protect Canadians from the harms of botnets. In deciding to establish the minimum standards applicable to the provision of network-level botnet blocking, the Commission is relying on market forces to the maximum extent feasible and interfering with the operation of competitive market forces to the minimum extent necessary to achieve the objectives. In its determination to establish guiding principles and a process for determining minimum technical parameters, the Commission is employing measures that are efficient and proportionate to the purpose of preventing the significant harm caused to Canadians by botnets. Furthermore, the botnet-blocking framework is intended to be technology-neutral and flexible to encourage innovation by carriers in addressing botnet communications. Finally, implementation of such a framework will advance the policy objectives set out in paragraphs 7(a), (b), (f), (g), (h) and (i) of the Act.[29]

Secretary General

---

[27] *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives*, SOR/2006-355, 14 December 2006

[28] *Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives to Promote Competition, Affordability, Consumer Interests and Innovation*, SOR/2019-227, 17 June 2019

[29] The cited policy objectives are: 7(a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions; 7(b) to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada; 7(f) to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective; 7(g) to stimulate research and development in Canada in the field of telecommunications and to encourage innovation in the provision of telecommunications services; 7(h) to respond to the economic and social requirements of users of telecommunications services; and 7(i) to contribute to the protection of the privacy of persons.

Related documents

- *Call for comments – Development of a network-level blocking framework to limit botnet traffic and strengthen Canadians' online safety*, Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9, 13 January 2021; as amended by Compliance and Enforcement and Telecom Notice of Consultation CRTC 2021-9-1, 29 June 2021

- *Application of regulatory obligations directly to non-carriers offering and providing telecommunications services*, Telecom Regulatory Policy CRTC 2017-11, 17 January 2017

- *Regulatory measures associated with confidentiality provisions and privacy services*, Telecom Regulatory Policy CRTC 2009-723, 25 November 2009

- *Review of the Internet traffic management practices of Internet service providers*, Telecom Regulatory Policy CRTC 2009-657, 21 October 2009

- *Competitive local exchange carrier access to incumbent local exchange carrier operational support systems*, Telecom Decision CRTC 2005-14, 16 March 2005

- *Confidentiality provisions of Canadian carriers*, Telecom Decision CRTC 2003-33, 30 May 2003; as amended by Telecom Decision CRTC 2003-33-1, 11 July 2003

- *Review of the general regulations of the federally regulated terrestrial telecommunications common carriers*, Telecom Decision CRTC 86-7, 26 March 1986

Appendix 1 to Compliance and Enforcement and Telecom Decision 2022-170

Guiding principles for a network-level botnet-blocking framework

Necessity

Blocking must be done exclusively for the purpose of cyber security[30] and not for any other purpose, including blocking otherwise illegal activity, or blocking for commercial, competitive, or political purposes.

Accuracy

Any impact on legitimate services must be as minimal as possible, limited to that which is necessary in order to achieve the objective of blocking the malicious traffic. The public must have the opportunity to report and resolve false positives and over-blocking in an effective and timely manner.

Transparency

Customers and prospective customers must be provided with clear information about the cyber security network-level blocking solutions applied by carriers. The information to be disclosed should provide sufficient information for Canadians to make informed decisions about which carriers they might wish to do business with, but should not be so detailed that it would undermine the effectiveness of the framework by providing actionable information to malicious actors on how to circumvent the blocking mechanism. In addition, carriers must maintain and file specific metrics with the Commission to allow for public disclosure of statistics regarding the uptake and effectiveness of the blocking framework.

Customer privacy

In addition to complying with their existing privacy obligations,[31] carriers should implement practices that enhance those obligations to account for the specifics of a blocking framework to provide the highest level of consumer privacy protection.

Accountability

Carriers should document and periodically review all their blocking systems used for cyber security purposes in order to verify that their blocking program works as intended.

---

[30] See the definition provided in Footnote 7.

[31] See the *Personal Information Protection and Electronic Documents Act* and existing Commission obligations regarding the protection of confidential customer information.

Appendix 2 to Compliance and Enforcement and Telecom Decision 2022-170

Summary of matters to be examined by CISC

Technical scope of the framework (i.e., what is blocked)

As set out in the Commission's decision above, given that the indicators of compromise (IOCs) used by cyber security specialists, including blocklist owners for the purpose of blocking traffic do not specifically identify botnets but rather identify, more generally, malware traffic or traffic suggestive of computer intrusions, it may not be practical to isolate botnet traffic through specific IOCs. The Commission considers on a preliminary basis that blocking other IOCs for the purpose of cyber security should, as a matter of policy, be subject to the same guiding principles. Any broader approach centred on IOCs must be extremely well circumscribed to avoid risks of the approach gradually broadening to include blocking for other purposes.

Questions for CISC

- Are there technical barriers to applying the same guiding principles to the blocking of all IOCs?
- Are the definitions of cyber security and IOCs cited in Footnotes 7 and 8, respectively, accurate? If not, CISC is asked to amend these definitions.

Stakeholders' responsibility – centralized blocklist option

As set out in the Commission's decision above, a centralized blocklist is the most efficient and effective option. With this option, an independent expert body such as, for example, the CCCS or CIRA could volunteer to be in charge of maintaining a baseline blocklist, including adding and removing identified IOCs to be blocked, assessing various other blocklists and adding them to the baseline list where appropriate, and making the baseline blocklist available to all TSPs.

Questions for CISC

- Is there an independent expert body, such as the CCCS or CIRA, that is technically willing and technically able to maintain a centralized blocklist for use by TSPs? Is there a forum or platform currently used by TSPs that can make this blocklist available to all TSPs and other stakeholders? If so, the Commission requests that CISC identify in its report these parties and the blocklist to be used.
- Would this independent expert body also handle false positive claims that may occur as a result of applying its blocklist and update the list accordingly? If not, who will handle these claims (e.g., TSPs) and how will the centralized blocklist be updated accordingly? Either way, how will the public submit false positive reports?

- Would TSPs and other stakeholders (e.g., cyber security experts and law enforcement agencies) have the technical ability to request the addition or withdrawal of specific IOCs to the list?

Stakeholders' responsibility – decentralized blocklist option

As set out in the Commission's decision above, as a supplement to a centralized blocklist or in place of a centralized blocklist if that is not a viable option, TSPs may use other blocking solutions to ensure cyber security in order to maintain flexibility and foster innovation. These solutions include the use of commercial blocklist providers, as long as they are accredited to meet certain requirements.

Questions for CISC

- Who will accredit third party blocklists to ensure compliance with the guiding principles established by the Commission (e.g., each TSP or a central organization)?

- What might be the relevant criteria for third party blocklist accreditation?[32]

- By what mechanism will the public be able to submit a false positive report to ensure third party blocklist providers update their list when appropriate?

- Are there any other practical considerations or requirements that should apply to the management and updating of third parties' blocklists? Would any stakeholder have the technical ability to request the addition or withdrawal of specific IOCs to all existing lists in use by all Canadian TSPs?

Blocking methods other than centralized or decentralized blocklists

As set out in the Commission's decision above, TSPs may implement other cyber security blocking initiatives (e.g., TSPs proprietary systems, practices such as standard service port blocking, and other recommended best practices).

---

[32] There are examples of prior established blocklist accreditation criteria, such as those defined by the Internet Corporation for Assigned Names and Numbers to establish the Reputation Block Lists used in the Domain Abuse Activity Reporting System: have longevity, have a track record within operational security communities, have ubiquitous use in public and private organizations, be subject to academic and industry scrutiny, and have suitably low false positive rates. Other possible criteria may include, for example, have experience maintaining botnet and malware blocklists, be certified by a reputable standards organization or be endorsed by appropriate industry professionals, and have service standards for taking action in response to a false positive claim.

Question for CISC

- Regarding other cyber security blocking initiatives, are there technical considerations or requirements that would be relevant for the Commission to consider?[33]

Other technical and implementation details

As set out in the Commission's decision above, network-level botnet blocking provided by TSPs should be applied by default so that customers do not have the option to either opt in or opt out, since this would undermine the purpose of the framework. However, there may be circumstances in which these options are necessary, such as a pilot phase during the implementation process.

Questions for CISC

- Is there a technical need to allow individual consumers to opt in or opt out of the network-level blocking system if it is implemented by their carrier (e.g., pilot phase during the implementation process)?

- What other technical attributes would maximize its uptake and effectiveness?

---

[33] Two of the Internet Engineering Task Force's best practices documents (Recommendations for the Remediation of Bots in ISP Networks RFC 6561 and Technical Considerations for Internet Service Blocking and Filtering RFC 7754) and the Broadband Internet Technical Advisory Group's Port Blocking Report may be relevant and facilitate CISC's recommendation of technical parameters.