Thursday, March 10, 2022
The Hague

Multistakeholder Imposition of Internet Sanctions

Executive Summary

The invasion of Ukraine poses a new challenge for multistakeholder Internet infrastructure governance. In this statement, we discuss possible sanctions and their ramifications, lay out principles that we believe should guide Internet sanctions, and propose a multistakeholder governance mechanism to facilitate decision-making and implementation.

Introduction

The Internet is in its thirtieth year of transition from national to multistakeholder governance. As we encounter pivotal moments, we must decide as a community whether Internet self-governance has matured sufficiently to address such newly encountered issue. Governments have imposed sanctions throughout history, but the global Internet governance community has not yet established a process dedicated to this task.

We believe it is now incumbent upon the Internet community to deliberate and make decisions in the face of humanitarian crises. We may not responsibly dismiss such crises without consideration, nor with consideration only for the self-interest of our community's own direct constituents; instead, maturity of governance requires that self-interests be weighed in the balance with broader moral and societal considerations. This document is the beginning of a global Internet governance conversation about the appropriate scope of sanctions, the feasibility of sanctions within the realm of our collective responsibility, and our moral imperative to minimize detrimental consequences.

Principles for Internet Infrastructure Governance Sanctions

We, the undersigned, agree to the following principles:

- Disconnecting the population of a country from the Internet is a disproportionate and inappropriate sanction, since it hampers their access to the very information that might lead them to withdraw support for acts of war and leaves them with access to only the information their own government chooses to furnish.

- The effectiveness of sanctions should be evaluated relative to predefined goals. Ineffective sanctions waste effort and willpower and convey neither unity nor conviction.

- Sanctions should be focused and precise. They should minimize the chance of unintended consequences or collateral damage. Disproportionate or over-broad sanctions risk fundamentally alienating populations.

- Military and propaganda agencies and their information infrastructure are potential targets of sanctions.

- The Internet, due to its transnational nature and consensus-driven multistakeholder system of governance, currently does not easily lend itself to the imposition of sanctions in national conflicts.

- It is inappropriate and counterproductive for governments to attempt to compel Internet governance mechanisms to impose sanctions outside of the community's multistakeholder decision-making process.

- There are nonetheless appropriate, effective, and specific sanctions the Internet governance community may wish to consider in its deliberative processes.

Recommendations

We believe it is the responsibility of the global Internet governance community to weigh the costs and risks of sanctions against the moral imperatives that call us to action in defense of society, and we must address this governance problem now and in the future. **We believe the time is right for the formation of a new, minimal, multistakeholder mechanism, similar in scale to NSP-Sec or Outages, which after due process and consensus would publish sanctioned IP addresses and domain names in the form of public data feeds in standard forms (BGP and RPZ), to be consumed by any organization that chooses to subscribe to the principles and their outcome.** This process should use clearly documented procedures to assess violations of international norms in an open, multistakeholder, and consensus-driven process, taking into account the principles of non-overreach and effectiveness in making its determinations. This system mirrors existing systems used by network operators to block spam, malware, and DDoS attacks, so it requires no new technology and minimal work to implement.

We call upon our colleagues to participate in a multistakeholder deliberation using the mechanism outlined above, to decide whether the IP addresses and domain names of the Russian military and its propaganda organs should be sanctioned, and to lay the groundwork for timely decisions of similar gravity and urgency in the future.

Signed,

Bart Groothuis, Member of the European Parliament, Netherlands
Bill Woodcock, Executive Director, Packet Clearing House
Ihab Osman, Non-Executive Director, Internet Corporation for Assigned Names and Numbers
Mike Roberts, founding President and CEO, Internet Corporation for Assigned Names and Numbers
Jeff Moss, President, DEFCON
Niels ten Oever, Postdoctoral Researcher, University of Amsterdam
Marina Kaljurand, Member of the European Parliament, Estonia, former ambassador to Russia and the United States
Eva Kaili, Member of the European Parliament, Greece
Runa Sandvik, security researcher
Kurt Opsahl, Electronic Frontier Foundation (affiliation for identification purposes only)
John Levine, President, CAUCE North America
Virendra Rode, founder and contributor, Outages.ORG
Stephen D. Crocker, Edgemoor Research Institute
Job Snijders, board member, RIPE NCC, PeeringDB, and Route Server Support Foundation
Moez Chakchouk, Director of Policy, PCH, former ADG/CI UNESCO and former Tunisian minister
Doug Madory, Director of Internet Analysis, Kentik
Ondrej Filip, CEO, CZ.NIC
Greg Rattray, Founder, Next Peak and former cybersecurity advisor to ICANN
Serge Droz, in personal capacity, Director FIRST
Mark Tinka, board member, FranceIX
Dmitry Kohmanyuk, founder, Hostmaster Ltd.
Timothy Denton, Chairman, Internet Society, Canada Chapter
Barry Greene
Perry E. Metzger, Managing Member, Metzger, Dowdeswell & Co. LLC
Roelof Meijer, CEO, SIDN
Svitlana Matviyenko, Associate Director, Digital Democracies Institute, Simon Fraser University
Rabbi Rob Thomas, CEO, Team Cymru
Harald Summa, CEO, DE-CIX
Chris Gibson, in personal capacity, CEO FIRST
Tom Killalea
The Internet Archive
Philip Reiner, CEO, Institute for Security and Technology
Megan Stifel, Chief Security Officer, Institute for Security and Technology
Bart Stidham, CEO, NAND Technologies
Rudolf van der Berg, Programme Manager, Stratix Consulting
Alejandro Pisanty, Professor, National Autonomous University of Mexico
Henrik Kramselund, CEO Zencurity Aps
Stéphane Duguin, CEO Cyber Peace Institute, in personal capacity

Annex: Technical Discussion of Internet Governance Sanction Measures

This statement is occasioned by the letter Andrii Nabok (Андрій Набок) of the Ukranian Ministry of Digital Transformation addressed to the Internet Corporation for Assigned Names and Numbers (ICANN) on the morning of Monday, February 28, 2022.[1] ICANN[2] and RIPE[3] replied to Mr. Nabok's letter directly, in the narrowest possible terms, and in the negative.

In this annex, we discuss the technical specifics of each of the proposed sanctions, as well as of other possible Internet sanctions which we suggest are more effective, more precise, and carry fewer risks and lower costs.

Analysis of Ukraine's Request

We respect Mr. Nabok's professional expertise and his inclusion of Ukraine's Internet community in the drafting of his letter in the full spirit of the multistakeholder principles by which the Internet is governed, and we express our deepest sympathies for the indescribable trauma Ukraine is experiencing as a result of Russia's invasion, which we condemn without reservation.

Mr. Nabok's letter requests the imposition of four Internet governance sanctions against Russia, namely:

- Permanent or temporary revocation of the country code top-level domains ".ru", ".рф" and ".su".
- Revocation of SSL certificates associated with those domains.
- Disablement of DNS root servers situated within the Russian Federation.
- Withdrawal of the right to use IPv4 and IPv6 addresses by Russian networks.

We commend Mr. Nabok and the Ukrainian people and government for responding to bloodshed with diplomacy and seeking deescalatory sanctions. Internet governance sanctions must, however, be selected and implemented carefully, in order to achieve the greatest effect and to avoid unanticipated consequences. In the attached appendix, we discuss each of the proposed sanctions, as well as others we consider more effective, with lower costs and risks of unintended consequences.

Revocation of country-code Top Level Domains (ccTLDs)

Every ISO-3166 Alpha-2 two-letter abbreviation of a national name is reserved for the use of the Internet community of that nation as a "country-code Top Level Domain," or "ccTLD." This reservation is made expressly for the Internet community of the nation and not the government of the nation. Geographic, political, and sociocultural allocations of "internationalized" top-level domains (such as ".рф" to the Russian Federation, or ".укр" to Ukraine) are made in parallel with the ISO-3166 mechanism.

The primary users of any ccTLD are its civilian constituents, who may be distributed globally and may be united by linguistic or cultural identity rather than nationality or national identity. Removal of a ccTLD from the root zone of the domain name system (the sanction suggested by the letter) would make it very difficult for anyone, globally, within Russia or without, to contact users of the affected domains, a group that consists almost entirely of Russian-speaking civilians. At the same time, it would have relatively little effect upon Russian military networks, which are unlikely to rely upon DNS servers outside their own control.

We therefore conclude that the revocation, whether temporary or permanent, of a ccTLD is **not an effective sanction** because it disproportionately harms civilians; specifically, it is ineffective against any government that has

---

[1] https://eump.org/media/2022/Goran-Marby.pdf

[2] https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[3] https://www.ripe.net/publications/news/announcements/ripe-ncc-executive-board-resolution-on-provision-of-critical-services

taken cyber-defense preparatory measures to alleviate dependence upon foreign nameservers for domain name resolution. In addition, any country against which this sanction was applied would likely immediately set up an "alternate root," competing with the one administered by the Internet Assigned Numbers Authority, using any of a number of trivial means. If one country did so, others would likely follow suit, leading to an exodus from the consensus Internet that allows general interconnection.

Revocation of certificates associated with domain names

At least two kinds of cryptographic certificates and signatures are potential mechanisms for sanction, and we discuss each independently. First, revocation of SSL certificates, as mentioned in Mr. Nabok's letter:

SSL ("Secure Socket Layer"), which has been succeeded by TLS ("Transport Layer Security"), is a certification mechanism principally used to authenticate and encrypt connections from web browsers to web servers. Such certificates are used in online commerce and banking, among other less visible roles. Certificates are issued by Certificate Authorities ("CAs"), of which there are many hundreds in existence,[4] a significant number of them are controlled, directly or indirectly, by national governments or intelligence agencies. Any one of these organizations may issue a certificate to anyone, certifying that they are the authentic administrator of any domain.[5]

The revocation of certificates associated with governmental or military domains is **not an effective sanction**, because the targeted government is likely already using a Certificate Authority under its own control, and if it is not it can easily cause any CA under its influence to issue a replacement certificate. The revocation of certificates associated with private subdomains (for instance, redcross.ru, citibank.ru) would render communications between these organizations and their constituencies insecure and vulnerable to cybercrime until they were able to get new certificates issued; decreasing law and order and rendering a civilian population more vulnerable to crime is **not an effective sanction**. Alternatively, adding existing certificates for propaganda outlets to Certificate Revocation Lists or using Online Certificate Status Protocol (OSCP) to flag them as revoked would warn casual users such websites are problematic and require them to take explicit action to proceed beyond the warning. These techniques are, however, limited: they must generally be done by the same CA that issued the original certificate, which may not be outside the influence of the sanctioned government. We thus believe this to be **a moderately effective sanction** in the cases where it is possible to invoke: it is specific, easily centrally implemented, and has little chance of unintended broader consequences. In X.509 public key infrastructures, certificate revocation cannot be rescinded; a new certificate must be issued and deployed.

Revocation of DNSSEC signatures on DNS delegations

The cryptographic signatures used to authenticate domain names are known as DNSSEC, or DNS Security Extension signatures. Clients can evaluate the veracity of the mappings between domain names and IP addresses, which is what allows them to find and connect to resources on the Internet, by cryptographically validating the DNSSEC signature associated with a domain name.

If a top-level domain were removed from the DNS root, the DNSSEC signature that validates the delegation of that domain would consequently be removed as well. DNS clients or resolvers still in possession of the old information could continue to reach the websites or email addresses identified by a domain, but they would be unable to validate that they had arrived at the right place. The DNSSEC signature validating the delegation of a top-level domain could also be removed while leaving the delegation itself in place.

DNSSEC signatures prevent criminals from performing "man-in-the-middle" attacks, impersonating the website of a retail bank, for instance, to capture the user's authentication information and empty their accounts. Military and high-security networks may use technical mechanisms to ensure that lack of a DNSSEC delegation above a

---

[4] https://www.eff.org/files/defconssliverse.pdf

[5] https://www.techrepublic.com/article/compromised-certificate-authorities-how-to-protect-yourself

signature under their control, in the DNS hierarchy, will not interfere with their resolution. Regular Internet users, however, either will be confronted with error messages indicating that their bank's website is an impostor or will not be notified if an attacker stands between them and their bank.

Removing the DNSSEC signature validating the delegation of a national top-level domain, whether in association with the removal of the delegation or not, may have little or no effect upon military and other high-security networks, but it would decrease law and order and make ordinary people much more susceptible to cybercrime. Tampering with DNSSEC signatures is thus **not an effective sanction**.

Disablement of DNS root servers

Root nameservers are simply those nameservers that hold a static copy of the DNS "root zone," which is, by its very nature, public information. Essentially any nameserver may be made a root nameserver, simply by telling it to retrieve and cache copies of the DNS root zone.

Disabling *specific* root nameservers has no effect, since they are, by design, not uniquely privileged or in possession of unique information. Disabling *all* root nameservers is not feasible since it would disable the Internet for everyone, and anyone could, and would, establish new ones. Disabling root nameservers thus has **no utility as a sanction**.

Withdrawal of the right to use Internet Protocol addresses

Internet Protocol (IP) addresses, the numeric identifiers by which Internet devices find each other, are allocated by the five Regional Internet Registries that together constitute the Number Resource Organization (NRO). Réseaux IP Européens (RIPE) is the Regional Internet Registry for Europe, the Middle East, and parts of Central Asia, with responsibility for allocating IP addresses to Russian entities. It is within RIPE's power, if directed to do so by its member organizations through its multistakeholder governance process, to create policy that would effectively withdraw the allocations of IP addresses it has made to Russian organizations.

This situation bears some similarities to the governance of domain names, yet it also contains crucial differences. ICANN's authority extends no further into the DNS hierarchy than the root level, so actions taken by ICANN inherently affect entire top-level domains unitarily, without the possibility of "surgical" actions upon one subdomain and not another. By contrast, the Regional Internet Registries can affect policy on a per-organization (or even finer) basis. Yet rescinding an IP address allocation does not prevent its previous holder from continuing to use it. Indeed, "IP address hijacking" is a relatively commonplace problem on the Internet. Therefore, although it can be precisely targeted, simply rescinding the right to use an IP address allocation is **not, by itself, an effective sanction**.

Note that this process of IP address revocation and RPKI attestation revocation would be a normal consequence of an address recipient (such as the Russian military) failing to pay annual registration fees to its Regional Internet Registry, something that may in fact come to pass as a consequence of financial and banking sanctions. But such a process might take years. Another negative consequence of revoking IP address allocations is that revoked addresses will likely be allocated to a different recipient subsequently, who will then find themselves competing with the original holder for their use.

Manipulation of routing security attestations

A potential sanction not explicitly requested in Mr. Nabok's letter is the manipulation of routing security attestations to produce the effect of a partial or complete disconnection from the Internet of specific networks, such as those of the Russian military or propaganda agencies.

As with domain names, technical mechanisms exist to cryptographically verify the legitimacy of use of IP addresses. Routing Policy Specification Language (RPSL) and Routing Public Key Infrastructure (RPKI) are the two primary such mechanisms. To be used for communication on the Internet, IP addresses must be "announced" through the routing system, and the routers of the larger and better-secured networks utilize these two mechanisms to ensure that

invalid routes are not used by their routers. Smaller and less-secured networks do not typically implement these mechanisms.

A manipulation of RPSL and RPKI records in centralized registries would flow through to all networks employing these common routing security mechanisms, some of which would then automatically stop routing traffic to and from the specified networks, without affecting other "adjacent" civilian networks or being subject to trivial "work-arounds."

The manipulation of RPSL and RPKI routing security attestations could be an effective sanction measure, because it appears precise, easily and quickly implemented and reversed, and reasonably effective. However, the appropriation of preexisting routing security mechanisms for use in sanctions, likely unexpected by the participating networks, could conflict with the business or regulatory requirements of those networks, and, crucially, could risk the withdrawal of networks from the system entirely. Such an exodus would both make this potential sanction less effective in the future and have the far greater cost of eroding cybersecurity for the Internet as a whole, the purpose for which the routing security systems were built in the first place. This thus **constitutes an unacceptable risk**.

Other Internet-associated, non-technical sanctions

Other sanctions related to the Internet's operation and governance may be worth considering. These include, for example, the disallowance of sanctioned personnel from participation in Internet governance, policymaking, or standardization proceedings. Such nontechnical measures are outside the scope of this document.

Blocklisting

Network operators and DNS resolver operators already make use of multistakeholder-governed lists, similar to the way financial lenders use credit scoring agencies, to determine what IP addresses to route and pass traffic between, and what domain names to resolve. This is the mechanism by which persistent spammers and address hijackers are excluded from the network, and by which Internet users are protected from malware and phishing attacks.

The technical mechanisms by which such blocking information is passed are mature, robust, instantaneous, and globally standardized. Information related to IP addresses and Autonomous System Numbers is mostly carried over BGP feeds, while information related to domain names is mostly carried over RPZ feeds. Both mechanisms are implemented by essentially all large operators globally. Blocklisting IP addresses and Autonomous System Numbers has all of the advantages of address block revocation or manipulation of routing security attestations, without the drawbacks. It allows network operators to block both the acceptance of routes and the passage of traffic, each or both of which may be appropriate in different situations and in response to different threats. Blocklisting of domain names allows full precision and specificity, which is the problem that precludes action by ICANN. The system is opt-in, voluntary, consensual, and bottom-up, all values the Internet governance community holds dear. Yet, at the same time, it has achieved broad adoption.

We conclude that the well-established methods of blocklisting provide the **best mechanism for sanctioning both IP routes and traffic and domain names**, and that this mechanism, if implemented normally by subscribing entities, has no significant costs or risks.

Our conclusion is that **blocklisting** of IP addresses, Autonomous Systems, and domain names upon which the multistakeholder community can establish consensus is effective and carries no inherent danger of being over-broad. Once decided upon, it is easily invoked—and equally easily rolled back once the problem is resolved. Most important, it carries no significant costs or risks and is aligned with the Internet's multistakeholder governance values and principles.

———