The Internet’s role in sanctions enforcement
Russia/Ukraine and the future

Bill Woodcock
DEF CON 30
August 12, 2022
As Russia invaded Ukraine in February of this year, the Ukrainian government sent requests to ICANN and RIPE to have Russia removed from the Internet.

Those requests were refused, but engendered a lively debate on the role of Internet operators and the Internet governance system in sanctioning bad actors, on the Internet and in the world.

I’ll be talking about how governmental and intergovernmental sanctions are defined and enacted, the Internet community’s reaction to past attempts to engage the Internet in sanctions enforcement, the current conflict, and what the Internet community is doing in this area to prepare for future conflicts.
Sanction basics

Governments devise and impose sanctions. A private party doing the same thing voluntarily is a boycott.

Sanctions don’t require that Internet governance be applied. Nor are they generally up for moral judgment. They’re a matter of compliance with national law.

Internet service providers are incorporated and do business in countries, each of which has national law, sometimes conflicting.

Where there are decisions to be made, they arise in the case of irreconcilable conflict between national laws.
Sanction basics

A sanction is a punitive measure which is deescalatory relative to kinetic conflict.

“Cyber sanctions” denote sanctions of any sort which are in retaliation for cyber-offense.

“Internet sanctions” denote sanctions imposed using Internet means in retaliation for any type of offense.

“Comprehensive sanctions” effect an entire country, and haven’t really been used for the past fifty years.

“Targeted sanctions” specify a particular entity, usually a person, corporation, building, ship, or airplane.
Sanction basics

Sanctions have three, non-exclusive purposes:

**Signaling** communicates a community’s disapproval to the sanctioned entity and the public: to convey to the world that an army is operating outside the bounds of legal armed conflict and this should not be tolerated, for instance.

**Constraint** is an attempt to directly curtail the actions of the sanctioned party: to stop a DDoS by blocking resolution of the domain name by which it locates its command and control, for instance.

**Coercion** is an attempt to influence the voluntary behavior of the sanctioned party: to convince an arms manufacturer to stop selling to a third party, for instance.
Governments:

> have thousands of years of experience using sanctions regimes as a deescalatory measure in times of conflict.

> have realistic expectations about the effectiveness of sanctions.

> have far less insight into the workings of communications networks than into the workings of financial networks.

> typically have little internal expertise in identifying the addressable Internet resources of sanctioned entities.

> are really, really, REALLY bad at publishing large datasets at well-known locations in harmonized machine-readable form.
Internet network operators:

> want to comply with sanctions regimes but often misperceive the scope and goals of sanctions.

> mostly aren’t subject to governmental regulation, don’t have “know your customer” regimes, and are unprepared to navigate sanction regulations.

> face a range of risks, including fines or criminal prosecution for over-under- or non-compliance or misapplication; and secondary effects of financial sector de-risking and customers seeking compensation for damages.

> often operate transnationally, and may face irreconcilable conflicts between compliance in one country and anti-trust or privacy laws in others.

> may be conflicted between protecting the network from bad actors and an ideological commitment to an “open Internet” blind to content or identity.

> are typically pretty skilled at blocking abusive behavior on the Internet.
German Bundesnetzagentur legal guidance:

> Blocking too early (before a decision) is illegal. Customers can insist on compensation (or sue for damages).

> Incorrect blocking (if the decision changes compared to the original) may be illegal in parts and allows claims for damages.

> Blocking that is not carried out is illegal and may be prosecuted by the public prosecutor's office.

> Overblocking (i.e. blocking more than the organisation subject to the sanction) is illegal and will be prosecuted by the BNetzA. Affected customers are entitled to damages.

> BNetzA sanction lists sometimes contain URLs, in which case only the specific web service is to be blocked; a DNS block can be overblocking.

> For the lists issued by the BNetzA, the BNetzA assures that it will not initiate legal proceedings against the ISP if overblocking occurs.
Welcome to the Internet Sanctions Project

This is an open, Internet community governed, project which produces real-time BGP and RPZ data feeds of network resources (IP addresses, Autonomous System numbers, and domain names) associated with sanctioned entities. These data feeds facilitate Internet network operators in complying with governmentally-mandated sanctions against violators of international and human rights law.

Why does this project exist?

Sanctions have been used as a tool of statecraft for thousands of years, but their use has become particularly widespread in the latter part of the Twentieth Century. Most sanctions used since the Second World War and until the start of the new Millennium were employed through the United Nations. Over the past 20 years, however, impasse at the United Nations Security Council (UNSC) has meant that a number of national governments and regional organisations also use their own autonomous (or unilateral) sanctions. These can supplement multilateral (UN) sanctions, or can be imposed entirely in their absence. All sanction regimes employed today are supposed to be “targeted” or “smart” (geared to only impact on certain targets and not a country’s entire population).

The United States (US) is the most prolific user of autonomous sanctions, followed by the European Union (EU). A number of other nations, such as the United Kingdom (UK), Canada, Australia and Japan also use autonomous sanctions; international organisations (such as the African Union and the League of Arab States) also employ them. Sanctions are also used to increase pressure on targeted governments to reverse policies that are seen as intimidating, repressive or aggressive in some way.

Sanctions can be economic (e.g., trade restrictions, freezing of assets, financial embargoes and suspensions of financial transactions) or military (e.g., the deployment of military forces, restrictions on arms exports).
Sanctions.NET project structure

A **policy** group monitors legally-binding sanction initiatives, evaluates sanctions for Internet implementation, and liaises with governments.

An **intelligence** group investigates and catalogs the Internet resources (IP addresses, Autonomous System numbers, and domain names) held by sanctioned entities.

An **oversight board** provides a final check on resources included in the blocking feed, verifying conformity with international and human rights law.

An **operations group** keeps the BGP and RPZ feed publishing mechanisms working and gathers feedback from implementers.

A **research group** is responsible for metrics and monitoring of the system and its effectiveness, and liaises with the academic community.
Where does the work stand now?

A best-practices standardization process is underway in the OECD, which should result in agreement between governments on a harmonized machine-readable format for sanctioned entity identifiers.

We are urging individual governments to determine that networks using the mechanism are compliant, and not over-compliant.

The technical mechanisms are proven but not integrated into production networks.

All of the working groups except the intelligence group are up and running.
Do sanctions disconnect anyone from the Internet?

No.

Internet sanctions remove the societal subsidy from the price paid by sanctioned entities to access the Internet.

In the same way that banking sanctions don't prevent sanctioned entities from using money, they just increase the friction and cost of doing so, Internet sanctions don't disconnect sanctioned parties from the Internet, they just ensure that they pay the full cost of using it, without the subsidies which would normally be provided as a function of societal cooperation.
When a sanctioned entity purposely uses resources shared with a non-sanctioned entity in order to evade a sanction, do we:

> let them get away with it, in order to avoid harm to an innocent third party, or

> block the third party as well, declaring the harm to be the moral responsibility of the sanctioned entity rather than the sanctioning body or implementer?

The human shield problem
The subdomain problem

When a domain name is sanctioned, should all subdomains of that domain be automatically sanctioned as well?

Or should each specific domain be sanctioned individually, recognizing that the operator of the sanctioned domain is then free to create additional as-yet-unsanctioned subdomains at will?
Conflicts with privacy and anti-trust law

Legal carve-outs frequently exist to ensure that protections in one area don’t conflict with higher priorities in another area.

Many countries have privacy laws which would treat all of the sanctioned-entity identifiers as legally-protected and heavily-regulated personally identifiable information (PII). A carve-out is needed to exempt sanctions implementors from PII regulation with regard to sanctioned entities.

Many countries have anti-trust law which prohibits competitors from collaborating to, for instance, deny service to specific entities. Banks use credit-scoring agencies to circumvent this for lending.
A similar carve-out is needed for sanctions implementors.
How does the beacon work?

The beacon is a set of IP addresses and domain names which are not used for connectivity by any real-world organization or users, which will always be "sanctioned" and can thus be used by researchers to measure the reach and effect of the system.

If the beacon is visible to you, the Internet sanctioning feeds are not being consumed by your transit providers or DNS recursive resolver operators.

Beacons are a frequently-implemented diagnostic feature of Internet routing security systems.
The sanctioned entity identifier morass

Transliterations are evil, Unicode is good.

Анато́лий
Anatoliy
Anatoly
Anatoli

Standard-but-often-abbreviated signifiers should be tokenized.

открытое акционерное общество
OAO
Open Joint Stock Company
Open Joint-Stock Company
Open JSC
OJSC
The right database schema will help (1 of 6)

All sanctions should be published in an XML schema which is standardized across all participating governments.

When governments wish to "inherit" one or more sanctioned entities, or a whole sanctions regime, from another government, an "inclusion by reference" external citation record should be used, rather than a new record created. Such a record should consist of the URL of the cited entity, a start date, and a (potentially empty) end date.

Each government should provide a single canonical well-known location, containing a single file with all currently-active sanctions imposed by that government regardless of agency and, optionally, separate files archiving expired sanctions by decade (i.e. one file covering January 1, 1980 through December 31, 1989) with sanctions assigned to files by date of imposition. (If a sanction lasted from May 1, 2009 through February 15, 2011, it would be recorded in the 2000-2009 file, not the 2010-2020 file.) A standardized naming scheme should be established based on the ISO 3166 Alpha-2 country code and the year range; for example, "sanctions-au-2000-2009.xml" or "sanctions-se-2020-present.xml"

Relevant metadata, like corporation type, gross revenue, gender of person, height and weight of person, should be recorded if available in standardized record types, in standardized (metric) units, with applicable date ranges and, if appropriate, source of authority or information.
The most authoritative name of any entity is the version as presented in its native language and script. Not transliterations. The native version should have a flag set which indicates it as such. Each transliteration should be flagged as an alias and labeled by the destination language/script. Names should be rendered in Unicode and labeled as to script and language.

Countries should be canonically indicated by their ISO-3166 Alpha-2 abbreviation where available, and a flag should be used to indicate when a country without an assigned ISO-3166 abbreviation is being identified.

Suffixes for companies, such as "LLC," "Joint Stock Company," "Corp," and prefixes and suffixes for people, such as "Jr.," "Honorable," "Eng.,” "Ph.D" should all be separated from the entity name proper, into separate corporate or individual prefix or suffix fields, and tokenized or harmonized to the degree possible.
Relationships between entities should be recorded using standardized forms ("subsidiary," "parent company," "controlling owner," "officer," "director," "father," "step-son," "spouse," with applicable date ranges and sources of authority or information where appropriate. Note that many relationships are asymmetrically bidirectional, and thus also require a directionality property: Aunt-Nephew for instance. It may be appropriate to use gender-neutral or gender-inclusive relationship names (i.e. use the same relationship to express father-daughter, mother-son, father-son, and mother-daughter) in order to avoid synchronization issues in cases of unknown or changed genders. Many types of relationships are possible, but this category should not be allowed to become overburdened: it may not be necessary to state that a sanctioned individual is the pilot of a sanctioned aircraft, for instance, when the individual and the aircraft are already related to a common sanctioned holding company by employment and ownership, respectively.
The right database schema will help (4 of 6)

For each name, dates of first and most recent observed use should be attached.

If an organization is dissolved, or a person dies, a date should be recorded.

For each sanction, a start date and, eventually, an end date should be attached to the entity-record, along with the identity of the sanctioning entity, and a link to a standardized identifier of the sanctioning event or reason. A single entity-record may have many separate sanction records attached to it, associated with different countries, different events, and different (possibly overlapping) date-ranges.

Sanctioning events or reasons should exist in their own table of unique records, including dates of general imposition or retraction, the entity which imposed them, and a canonical reference to the law, regulation, or finding in which the sanction is documented. The dates attached to the overall event need not be specific to the date level, and need not align exactly with the specific dates on which individual entities were added to the sanction. Each act of national law or regulation which produces a sanction list, whether new or an amendment to an existing list, should be represented as a unique record, with the national legal action being the unique identifier.
A table of meta-sanctioning events should be used to link national sanction events. For instance, a meta "Russia-Ukraine conflict" event with a start date of 2014 might be used to tie together many separate national sanctions imposed by different countries with date ranges 2014-present, 2014-2014, 2014-2015, 2021-present, 2022-present, et cetera.

People names should be separated into parts, and each part should be flagged with an order-of-rendering and a type: "given name," "patronymic," "family name," "anglicization," "nickname," etc.

The form of a personal name as it appears on a passport issued by the person's native country should have primacy. Other forms of the name should be flagged as aliases.

The most-commonly-used form of a personal name should be flagged as such.

All known identifying numbers (corporate registration numbers, Legal Entity Identifier (LEI), DUNS number, passport numbers, driver's license or ID numbers) should be saved, along with start and end dates of validity, date of issuance, name and location of issuing authority, etc.
Identification-issuing authorities should exist in their own separate table of unique entities, with aliases, most-commonly-used-form, structured place names, start and end date of authority, and hierarchical relationship to parent organizations.

When Internet resources are associated with sanctioned entities, they should exist in their own unique tables of IP address, Autonomous System Number, and Domain Name. Each resource should have a start (and potentially end) date which indicates its creation and deletion dates, not the dates at which it was associated with a sanctioned entity. These resources are then linked to sanctioned entities through a table of links, each of which contains, minimally, a unique identifier, pointer to source of authority, sanctioning event or reason, date of record creation, party or process which created the record, start date of link applicability, optional end date of link (or still-in-effect), as well as the unique identifiers of the sanctioned entity and the Internet resource. These links are potentially many-to-many, and multiple links may exist between the same pair of sanctioned entity and resource, at different or overlapping date ranges.
Questions
Discussion
Etc.?

Bill Woodcock
woody@pch.net