The ITU treaty provisions for infrastructure protection:
How they came to be and why they are relevant today

by Anthony M. Rutkowski [1]

Foreword

One of the most significant provisions today in contemporary international telecommunications law dealing with cyber security and infrastructure protection arose almost by chance in 1988. This provision is known as Art. 9.1b in a treaty instrument called the *International Telecommunication Regulations*, and obligates countries to "avoid technical harm to the operation of the telecommunication facilities of third countries" for internets spanning national boundaries. Such obligations potentially include setting and adopting standards, monitoring traffic flows, cooperation among parties, establishing implementing national laws, and instituting enforcement mechanisms.

The 9.1b provision was added during negotiations at a formal treaty making conference whose principal purpose was to create a treaty for public telecommunications and internet infrastructures. A major aim was to allow for the first time, the transnational interconnection of open national internet facilities for service to the public. The infamous Morris Worm incident occurred just a few weeks prior to the conference. It was the first significant attack within the DARPA-NSF internet infrastructure and resulted in virtually their entire internet at that time ceasing to function.

As a result of this first dramatic failure of internet infrastructure, the Art. 9.1b provision was crafted to effect an obligation among signatory nations that if they allow transnational internet capabilities, they are under a cyber security obligation to take steps to avoid technical harm. This short paper on the occasion of the ITU's Meeting on Cybersecurity in June 2005, describes this historic cybersecurity law development 17 years earlier.

Drafting a Treaty for Public Digital Internets

During the late 70s and early 80s, digital internet technologies moved forward rapidly. Quickly the Integrated Services Digital Network and X.25 packet networks evolved to encompass internet technologies and applications. This led to the creation of large scale industry standards initiatives in the ITU and other

---

[1] At the treaty making conference which adopted the International Telecommunication Regulations, Mr. Rutkowski was a senior member of the ITU staff and headed the conference secretariat in his capacity of Chief of International Telecommunication Regulations. During the six years preceding the treaty conference, as a senior staff member of the Federal Communications Commission associate professor at New York Law School and research associate at MIT, he wrote numerous published papers on this treaty as an instrument of public international telecommunication law for emerging new digital networks. He is now VeriSign, Inc. Vice President for Regulatory Affairs in Dulles, Virginia, USA, and participates in many domestic and international infrastructure security and law enforcement support activities.
The views expressed are purely personal, and in deep respect and gratitude to some of the people mentioned in this paper – who have played largely unrecognized, profoundly important roles in developing and protecting the global public internet infrastructures.

major standards bodies to develop the Open Systems Interconnection (OSI) suite of specifications and administrative arrangements.

Against this background of technology development and industry activity, discussions emerged between 1980 and 1982 on a new generic treaty instrument for digital internets that culminated in a consensus at the 1982 Plenipotentiary Conference "…to establish…a broad international regulatory framework for all existing and foreseen new telecommunication services." [2] Over the next several years, these discussions became a reality in setting a definitive treaty conference timetable for late 1988.

Much of the vision in driving this historical event is owed to former ITU Secretary-General Richard Butler of Australia, who understood the critical need for a global treaty for the new internet world comprised of competitive distributed facilities and services – including even broadband home networks that were becoming feasible at the time. In the mid-80s, he took the unusual step of working with the first organized group of lawyers focusing on digital internet law organized by one of the most respected legal scholars, the late Anne Wells Branscomb, and implemented ITU-sponsored meetings of international legal experts to consider the emerging issues and publish the first book on the subject.[3] As the treaty conference approached in 1988, technical experts and national monopoly providers found it difficult wrestle with the far-reaching new open network, competition, and internet legal issues. In response, he formed his own staff brainstorming group, and reached out to International Bar Association, European regulators, and even hosted special preparatory meetings in Geneva.[4]

For arcane historical reasons, the conference was denominated the *World Administrative Telegraph and Telephone Conference* (WATTC) notwithstanding the Secretary-General's attempt to adopt a more appropriate name by the ITU's interim governing Council. Its output treaty instrument was the *International Telecommunication Regulations*.

In the years and months leading up to December 1988, numerous preparatory meetings and collaborative activities led to a draft of an essential, minimal set of provisions for digital internetworking for the foreseeable future. These provisions were not surprising as the basic international arrangements for public communication network infrastructures tend to be quite similar whether the technology platform is the electrical telegraph, satellite systems, or internet protocols. The key features include agreement on a common purpose in establishing globally internetworked public networks and services, the role of government in assuring availability, the adherence to some common technical and operational standards, national security considerations, sharing information,

---

[2] Resolution No. 10, International Telecommunication Convention (Nairobi, 1982).

[3] *See, Legal Symposium on International Information Networks*, 4th World Telecommunication Forum, Geneva, 28-29 Oct 1983; *Law, Regulation, Standards of Global Communications*, World Telecommunication Forum, Washington DC, 18-19 April 1985; Anne W. Branscomb, editor, **Toward a Law of Global Communications Networks**, Longman, 1986.

[4] *See, e.g.*, ITU Secretary-General, *Global Interconnection and the Search for a New International Framework*, Deregulation in the 1990s, Paris, 8 Mar 1988; *Analysis Outline, International Telecommunication Regulations*, ITU Preliminary Consultations on WATTC-88, Geneva, 7-8 April 1988; Consultations on WATTC-88, Geneva, 11-12 April 1988.

prioritization of emergency communications, and settlement mechanisms among providers.[5]

What was new in the draft treaty was a unique provision that for the first time allowed the interconnection of open computer networks and making the services on those networks available to the public, free from traditional common carrier regulations. These innovative provisions were included in multiple sections of the treaty, especially a "special arrangements" article allowing for internets.

Rule No. 1: Protect the Infrastructure

It is worth noting that since the inception of intergovernmental telecommunications collaboration in 1850 at Dresden, the protection of public communication network infrastructures has been "rule no. 1." All cooperating nations have a shared obligation to maintain and protect the public communication infrastructure.[6] This rule spans not only wireline networks, but also all radiocommunications. The most basic underlying foundation for international cooperation on radio is the avoidance of harmful interference to the signals of other authorized radio stations.[7]

This obligation to protect the infrastructure has typically been implemented through several basic requirements. For 155 years, one requirement has always been fundamental. **Every signatory nation has an obligation to implement administrative and enforcement mechanisms whereby those who can cause harm to the network infrastructure or radiocommunications of another country can be authoritatively identified and contacted, to make that information available to other signatories, to take actions to mitigate the harm, and pursue the party causing the harm whether by accident or intent.**

During the 1980s, industry experts and especially the visionary internet naming, email, and mobile code pioneer Jim White, had met for several years in IFIP's Working Group 6.5 and the ITU's CCITT devising a highly innovative, authenticated internet name system based on hierarchical domains for all providers, subscribers, network management, and code distribution.[8] (The DARPA internet community would later implement a version of this hierarchical domain name system that is in common use today.)

In the early 70s, Jim White - who was extraordinarily productive in the initial DARPA internet academic and research community dealing with distributed and remote processing - understood well the challenges of open networks allowing

---

[5] *See, e.g., General Principles to Be Used as a Basis for Formulating International Telecommunication Regulations*, Doc. 5, World Administrative Telegraph and Telephone Conference, Melbourne 1988.

[6] *See, e.g.*, Art. 22, Interruption of communication, State Treaty Between Austria, Prussia, Bavaria and Saxony on 25 July 1850 concerning the establishment of the German-Austrian Telegraphic Union, Dresden; Art. 2, Convention Télégraphique International de Paris, Réglement de service international, Paris, 1865.

[7] *See* Arts. V, VI, *Protocol Final*, Conférence Préliminaire Concernant la Télégraphie Sans Fil, Berlin, 1903.

[8] James E. White, **A user-friendly naming convention for use in communication networks**, Proc. of the IFIP WG 6.5 working conference on Computer-based message services, Elsevier North-Holland, Inc. New York, NY, USA, 1984. *See also*, ITU-T Rec. X.500, *Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services*; ITU-T Rec. F.500, *International public directory services*.

nomadic users and mobile code. He had conceived and written the standards for Remote Procedure Calls (RPC), remote access (telnet), file transfers, email and resource sharing.[9] Leading dozens of other industry experts working in the CCITT at the time, he knew what it took to maintain and protect open public internet infrastructure. Together they instituted a combination of technical and administrative standards for implementation by every nation. As the provisions of the 1988 treaty began to come together, the use of these infrastructure protection mechanisms were assumed, and written into the fabric of the draft treaty by reference.

Enter the Morris Worm

Technical experts in the industry were aware during the 1980s that private internets were being developed by the U.S. Defense Advanced Research Projects Agency (DARPA), and were beginning to be used on an expanding scale by academic institutions. Their expansion in the U.S. was fostered by being excluded from any regulatory oversight or infrastructure obligations as private networks. This occurred in large measure because the legendary head of DARPA during the 70s who had championed the development of internet technology, Dr. Stephen Lukasik, subsequently went to the FCC and played a leading role in getting computer networks generally excluded from any regulation or imposed obligations under what became known as the *Computer II* policy.

By 1987, it was not uncommon for industry research engineers to be connected into the DARPA internet, especially as it began to expand with the infusion of hundreds of millions of dollars of National Science Foundation grants to both industry and academic institutions. By the time of the ITU telecommunications treaty conference in late 1988 the DARPA-NSF internet consisted of about 60,000 connected hosts and increasing at better than 100% per year.[10] Some extraterritorial extensions of the largely U.S. infrastructure existed – primarily through a few major defense and scientific related research facilities in other countries.[11]

Just after 18.00 hours on 2 November 1988 – three weeks before the start of the international treaty conference – essentially the entire DARPA-NSF internet

---

[9] *See, e.g.*, J. E. White, *Specifications for network use of the UCSB On-Line System*, RFC74, Oct 1970; J. E. White, *Network Specifications for Remote Job Entry and Remote Job Output Retrieval at UCSB*, RFC105, Mar 1971; J. E. White, *Network specifications for UCSB's Simple-Minded File System*, RFC122, Apr 1971; J. E. White et al., *The Data Transfer Protocol*, RFC171, Jun 1971; J. E. White, *User Telnet - description of an initial implementation*, RFC206, Aug 1971. J.E. White, *Telnet access to UCSB's On-Line System*, RFC216, Sep 1971; J. E. White et al., *Revision of the Mail Box Protocol*, RFC278, Nov 1971; J.E. White, *Request for network mailbox addresses*, RFC510, May 1973; J.E. White, *Proposed Mail Protocol*, RFC524, Jun 1973; J.E. White et al., *Standardizing Network Mail Headers*, RFC561, Sep 1973; J.E. White, *High-level framework for network-based resource sharing*, RFC707, Dec 1975; J.E. White, *Elements of a Distributed Programming System*, RFC708, Jan 1976. Jim White would later develop the first commercial mobile code operating system – Telescript - while at General Magic. *See, e.g.*, Peter Domel, *Mobile Telescript Agents and the Web*, IEEE Computer Society, *Compcon*, p. 52, 1996.

[10] *See* administrative and host count records of Hostmaster, DDN Network Information Center, SRI International.

[11] In Nov. 1988, 26 countries outside the U.S. had some form of Internet connectivity: Argentina, Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Iceland, Ireland, Israel, Italy, Japan, Korea, Malaysia, Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Thailand, United Kingdom. *Ibid*.

infrastructure unexpectedly shut down within a matter of a few hours. Some connected networks like MIT's managed to disconnect as they detected that something was propagating across the entire DARPA internet infrastructure.

In a kind of real-life replay of Watergate investigative journalism in the 1970s, a young technology reporter on the staff of the New York Times by the name of John Markoff undertook to discover what had happened. Day after day he wrote front page articles carried in major U.S. and international newspapers. (See the appended Annex of Markoff articles.) The public was fascinated that a supposedly failure-proof national network could fail so completely, so fast. Network technologists were particularly anxious, since the public telephone network's new signaling system and the OSI network protocols were based on the same technology.

Investigators discovered that a single graduate student by the name of Robert Tappan Morris – who was experimenting with the replication of computer code – had unintentionally acted alone and brought down the entire network research infrastructure. Adding to the intrigue was the irony that John Markoff's own version of "Deep Throat" turned out to be a senior scientist at the U.S. National Security Agency who happened to be Morris' father.[12] The particular kind of malicious code ultimately was dubbed the *Morris Worm*, and the precursor of a whole new world of both malicious viruses as well as unintended code failures capable of causing widespread collective and individual harm on internets.

One of the elegant features of Jim White's ITU-T internet domain name system – even though only partly implemented - is the ability to authenticate many kinds of network objects, including code. It remains today the primary means for leading vendors of software and network management code modules to authenticate their products.[13] A meta-namespace emerging from the WWW community known as Universal Resource Names now encompasses the ITU-T namespace.[14] All of these namespace include the ability to authoritatively identify a responsible party for a network object or code that emerged out of White's seminal work in IFIPS and ITU-T – a fundamental requirement for the protection of all open public network infrastructures

---

12 *See* John Markoff & Katie Hafner, **Cyberpunk**, Touchstone, 1991.

13 See ITU-T X.509, *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. *See also*, X.650 *et seq*, *Information technology - Open Systems Interconnection - Basic Reference Model: Naming and addressing*; X.667, *Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components*; X.669 *et seq.*; *Procedures for ITU-T registration of identified organizations*; X.680 et seq., *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*. There is a large body of material on major vendor sites such as Microsoft, Sun, and others concerning their support of X.509 certificates and code signing.

14 *See* Berners-Lee, T., *Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web*, RFC 1630, June 1994; Sollins & Masinter, *Functional Requirements for Uniform Resource Names*, RFC 1737. December 1994.

A New Treaty Framework for Electronic Communications

At the end of November 1988, representatives of 113 nations gathered in Australia at the elegant old Melbourne Town Hall for the treaty making conference on international telecommunications. As they arrived "down under," they received the proposals of the USSR administration that had just been submitted on 24 November – just four days before the opening of the conference, and were translated and reproduced on the 27th. Of significant interest was the USSR acceptance of the key provision on allowing international internets crafted through Secretary-General Butler's coordination. What they had also done, however, was to insert a key caveat in their proposed text – "on condition of no harm to third countries." [15]

This proposed USSR condition was innovative. Although other provisions dealt with harm potentially resulting from attaching unregulated terminal equipment, no one had previously dealt with harm arising from traffic on transnational internets. Subsequent discussions between the USSR delegation leadership and ITU conference officials made it clear that the provision was a direct response to the Morris Worm incident.

As the conference got underway, even Secretary-General Butler didn't anticipate just how difficult it would be to get global agreement on a common treaty arrangement for legacy telecommunication networks and the new world of internets. Conservative national regulatory authorities and government ministries of legacy monopoly networks came face-to-face with the reality of competitive computer networking.

During the initial days of the conference, heads of some conference delegations began filibustering the conference sessions railing against the notion that networks "outside the club" could be integrated into global internets to be provided to the public. The subject of invective was the provision of the draft treaty that Butler had encouraged through a combination of vision and diplomacy that allowed for the first time not only for transnational internets to be accessible by the public, but also for application service providers other than approved common carriers.

After several initial days of unproductive rancor among delegation heads prior to the conference, the Australian government borrowed its most skilled international diplomat – the late Dr. Peter Wilenski – who was named chairman of the treaty conference. Wilenski was extraordinary in getting contentious factions to work together in several decades of U.N. agency settings, and saved the conference from ending in either a stalemate, or worse yet - with provisions that even more explicitly banned the existence of transnational internets available to the public. Several years later Wilenski would become Australia's U.N. ambassador.

---

[15] *See* Proposal URS/40/5, *USSR, Proposals for the Work of the Conference*, Doc. 40, World Administrative Telegraph and Telephone Conference, Melbourne 1988.

The ITU's Infrastructure Protection Provision for Internets

As the negotiations under Wilenski's chairmanship got underway, one of the principal issues of the conference began to surface – the potential for substantial damage to public network infrastructures by making them more open. These concerns were articulated in several proposals going to network terminal attachments, in the USSR internet-related proposal, and in countless interventions by national delegations.

The dialogue on these contentious subjects – new services available to the public, new kinds of operators, internets, harm to the infrastructure – all played out through long Working Group C sessions running day and night during the first several days of the conference. Finally, Chairman Wilenski formed an Ad Hoc Group of the Plenary to resolve the issues and achieve an acceptable solution. On the morning of Friday, 2 December 1988, at 9:21 AM, the matter came to a head at the 3rd meeting of the Group.

The first intervention was that of Brazil who urged that the USSR text combined with that of France and Japan and serve as part of a "common ground" agreement among a number of delegations on allowing internet access to be made available to the public. During the next hour, 20 developed and developing countries in succession all supported the proposition. The chair called for a coffee break. When everyone convened 40 minutes later, the chair asked the USSR to prepare the final text by the next day and to provide additional detail on their infrastructure protection clause. The USSR delegate explained what had already been discussed privately about the Morris Worm, and described it to the conference as "some kinds of traffic could damage the facilities of third countries," and that this "was an important legal point."

For the rest of the morning session of the Ad Hoc Plenary Group, and on into the afternoon following lunch, the consensus building and text adjustments moved forward. Much of dialogue revolved around the nature of the obligations – both technical and administrative – to enhance infrastructure protection. For the most part, however, the infrastructure protection requirements for internets were cast at the 3 Dec 1988 meeting. The most significant subsequent change was the introduction of the word "technical" in the phrase "technical harm" to ensure that the obligations did not encompass economic harm. Lukasik notes that today, "while the original idea was to separate technical harm from economic harm, in the current context of cyber attacks the difference is meaningless. Technical harm is intended to cause economic harm, not just make computers stop working."[16] The observation underscores the contemporary need for effective definition, implementation, and continuing evolution of the original intergovernmental obligations under Art. 9.

[16] S.J.Lukasik, private note, 6 Jul 2005.

The resulting treaty provisions read:

Article 9
Special Arrangements

¶ 58 9.1 a) Pursuant to Article 31 of the International Telecommunication Convention (Nairobi, 1982), special arrangements may be entered into on telecommunication matters which do not concern Members in general. Subject to national laws, Members may allow administrations [or recognized private operating agency(ies)] or other organizations or persons to enter into such special mutual arrangements with Members, administrations [or recognized private operating agency(ies)] or other organizations or persons that are so allowed in another country for the establishment, operation, and use of special telecommunication networks, systems and services, in order to meet specialized international telecommunication needs within and/or between the territories of the Members concerned, and including, as necessary, those financial, technical, or operating conditions to be observed.

¶ 59 b) Any such special arrangements should avoid technical harm to the operation of the telecommunication facilities of third countries.

¶ 60 9.2 Members should, where appropriate, encourage the parties to any special arrangements that are made pursuant to No. 58 to take into account relevant provisions of CCITT Recommendations.

At the end of the Conference, all 113 participating countries signed the provisions. The Secretary-General crafted a press release highlighting the major issues and accomplishments of the treatymaking conference as encompassing arrangements for "the provision of international services to the public provided both by the traditional network operators, as well as the new entrants and organizations."17 Two highlighted results were:

> The Conference also laid down responsibilities for reciprocal cooperation between Members, should difficulties arise when services are provided by a foreign operator in a particular country.
>
> Special recognition was given to Members allowing administrations, recognized operating agencies or other organizations or persons to enter into arrangements with counterparts so allowed in another country for the establishment of special telecommunications networks, systems and services to meet special international telecommunication needs. As an extension of the very general "special arrangement" provision of the International Telecommunication Convention (Article 31), the Conference, in recognizing concerns of sovereignty, endorsed the role of mutually agreed special arrangements that would include, as necessary, the agreed financial, technical and operations conditions to be observed by all the parties concerned. These special arrangements should avoid technical harm to operation of the telecommunication facilities of third countries. This concept of "technical harm" had existed for many years in the Radio Regulations, but had not been necessary for specific and dedicated networks.[18]

---

17 ITU Press Release, *Historic International Conference Concludes Treaty Which Will Benefit All Providers of International Telecommunication Services Networks And Systems as Well as Users of Telecommunications Worldwide*, NP/88-6, 22 December 1988.

18 *Ibid*.

Implementing the Treaty Provisions

In the years immediately following the 1988 Conference, most countries gave serious attention to fulfilling their obligations under the new treaty which subsequently entered into force on 1 July 1990 among most of the world's nations. For the most part, the infrastructure protection components involved the application of relevant CCITT Recommendations relevant to the two principal internets – the international signalling system and the Open Systems Interconnection (OSI) based internets.

In 1995, however, the private DARPA/NSF IP research internet infrastructure was made available generally to the public, and largely eclipsed OSI internet platforms in the marketplace. The OSI authentication and network management technology, together with some its comprehensive domain name system and some X.400 based email system islands in government agencies, remain successful and span all internet infrastructures. However, it is IP internet infrastructure that has expanded on a much larger scale rather than OSI based infrastructures. In the process of this evolution and expansion, the application of the 1988 treaty provisions on infrastructure protection were largely ignored.

This state of affairs began to greatly concern some of the leaders who had played such a key role in the 70s and 80s in sponsoring and evangelizing internet technology and related regulatory forbearance regimes – especially Lukasik. Operating initially through Stanford University's prestigious Center for International Security and Cooperation (CISAC), Lukasik worked with an array of critical infrastructure and national security leaders and legal scholars such as Seymour Goodman, Ron Lehman, and others to create an ongoing program designed to rectify the already growing problems of the original DOD research platform becoming public infrastructure.[19]

Not surprisingly, much of the CISAC focus was similar to the substantive dialogue at the ITU 1988 treaty conference giving rise to the International Telecommunication Regulations, and some of the envisioned remedies were similar. Other internet intergovernmental infrastructure protection needs, however, went considerably beyond those within the scope of the ITU, and resulted several years later in the formation of provisions within the Convention on Cybercrime.[20] Still other needs – such as intergovernmental mechanisms for real-time incident response have yet to find effective solutions. Lukasik's holistic intergovernmental metaview encompasses several different elements of an Agency for Information Infrastructure Protection.[21]

---

19 *See, e.g.,* Stephen J. Lukasik, *Public and Private Roles in the Protection of Information-Dependent Infrastructure* (CISAC, May 1997); *Workshop on Protecting and Assuring Critical National Infrastructure*, (CISAC, July 1997). Some of this work was jointly done with the Center for Global Security Research at Lawrence Livermore National Laboratories. It is now sponsored by the Georgia Tech Information Security Center (GTISC). *See* <http://www.gtisc.gatech.edu/>

20 *See* Sofaer, Goodman, Cuéllar, Drozdova, Elliott, Grove, Lukasik, Putnam, & Wilson, *A Proposal for an International Convention on Cyber Crime and Terrorism*, The Hoover Institution, Consortium for Research on Information Security and Policy, and the Center for International Security and Cooperation, Stanford University, Aug 2000; *Convention on Cybercrime* (Budapest, 2001), COE Treaty Series 185.

21 *See* S. J. Lukasik, *What Does an AIIP Do?*, May 2000.

The ITU's Infrastructure Protection Provisions in the 21st Century

Seventeen years after the establishment of infrastructure protection provisions in the International Telecommunication Regulations at Melbourne, there seems to be a newfound, growing appreciation for the subject. Growth and innovation are being balanced with Rule No. 1 – protecting the infrastructure. At global, regional and national levels, technologists and lawmakers in industry and government are working together to understand and fashion Next Generation Network infrastructure protection frameworks and capability requirements.[22] There is a collective realization that there is something worse than not having the latest broadband infrastructure – it is having no infrastructure at all when it ceases to function across the entire nation, especially during times of emergency.

Not surprisingly, much of the focus now ongoing on Next Generation Networks technical standards, administrative requirements, and mandated regulatory requirements all deal with the management of authenticated identities of network providers, users, and objects through a common intelligent architecture.[23] Today, a single anonymous nomadic user of a broadband Internet "pipe" – whether provider or subscriber - can access enormous network resources and adversely affect millions of other users or even the entire infrastructure.

The core international requirements for infrastructure protection are pretty much the same as they have always been:

1) global intergovernmental agreement to avoid harm to another country's network infrastructure, and

2) implementation of effective administrative and enforcement mechanisms whereby those who can cause harm to the network infrastructure or radiocommunications of another country can be authoritatively identified and contacted, to make that information available to other signatories, to take actions to mitigate the harm, and pursue the party causing the harm.

In addition to the internet infrastructure protection requirements in the ITU's International Telecommunication Regulations, the Convention on Cybercrime requires the same result. The obligations and needed capabilities are basic, simple and readily capable of implementation. Most significantly, they are urgently needed by all the diverse parties in government and industry who ultimately are responsible for the operating the infrastructure, ensuring its protection, and pursuing actors who cause harm either maliciously or unwittingly.

If there is any doubt whatsoever concerning exactly what is needed, the capabilities at a minimum should include those in the figure below. These capabilities are not entirely cost free, but they are minimal regulatory impositions, critically-necessary for national infrastructure protection and other essential public needs, and even potentially able to earn revenue for providers, such as authenticated calling/messaging name verification service options.

---

22 *See, e.g.*, Wenger & Metzger, *Critical Information Infrastructure Protection*, Center for Security Studies, ETH Zurich, 2004.

23 *See, e.g., Rapid Resolution of ITU-T Identifiers for NGN*, Doc. COM 17 – D 10, ITU-T Study Group 17, meeting at Moscow, March 2005.

Minimal Obligations for Infrastructure Protection and Justice Cooperation under the International Telecommunication Regulations and the Convention on Cybercrime Treaties

For all providers of communication services capable of adversely affecting services or subscribers in an other country:

- Sharing among administrations
  - current trusted provider identity and contact information
  - the ability to associate such providers with their services
- Ability to discover between administrations
  - current trusted associations between subscribers and the communication identifiers (e.g., phone number, IP address, etc) that providers use for their services to those subscribers
  - instant trusted resolution of minimal (i.e., non privacy sensitive) identifier associations

There are no other options here. The global public communications infrastructure today is facing challenges never experienced by any network or radiocommunication infrastructures in the past. The harmful activity can be almost instantaneous on very large scales, and the adverse effects can have significant national or industry sector economic implications over short periods of time, or effects that persist for a long time such as identity theft.[24] As Lukasik notes, the legacy ITU harmful interference mitigation and containment regime crafted over many decades may have implicitly evolved (or needs to evolve) to assume some of attributes of an arms control regime.

In some instances, the activity may have life-and-death consequences. Those in industry and government who are investigating or relying on the infrastructure, need to "resolve" identifiers to trusted information in milliseconds, and be able to act further to get current, trusted details in seconds. The minimal obligation capabilities described above underpin and enable almost every requirement that nations and their citizens expect from their public communications infrastructures.

The treaty provisions exist. The needs certainly exist. The Next Generation Network technical standards communities are active worldwide developing and identifying the needed architectures and standards. Regulatory, justice, and homeland security agencies worldwide are contemplating how to proceed with IP enabled NGN infrastructure and what capabilities to require. It's now time for industry and government together to begin acting in their common interest to protect their nations' public communication infrastructure and the people that use it.

[24] Stephen J. Lukasik, *Protecting the global information commons*, 24 Telecommunications Policy (2000) at 519. Ref. <http://www.csupomona.edu/~gurey/urp337/telecom.pdf>

ANNEX

Unfolding History of the Morris Worm in the New York *Times* November 1988

4 Nov 1988	'Virus' in Military Computers Disrupts Systems Nationwide, The New York Times, November 4, 1988, Friday, Late City Final Edition, Section A; Page 1, Column 4; National Desk, 1138 words, by John Markoff
5 Nov 1988	Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security, The New York Times, November 5, 1988, Saturday, Late City Final Edition, Section 1; Page 1, Column 1; National Desk, 1629 words, by John Markoff
6 Nov 1988	Whiz's mistake brought life crashing down, St. Petersburg Times (Florida), November 6, 1988, Sunday, City Edition, NATIONAL; Pg. 1A, 1216 words, by John Markoff
6 Nov 1988	How a Need for Challenge Seduced Computer Expert, The New York Times, November 6, 1988, Sunday, Late City Final Edition, Section 1; Part 1, Page 1, Column 1; National Desk, 1462 words, by John Markoff
7 Nov 1988	Computer Invasion: 'Back Door' Ajar, The New York Times, November 7, 1988, Monday, Late City Final Edition, Section B; Page 10, Column 4; National Desk, 1271 words, by John Markoff
8 Nov 1988	Living With the Computer Whiz Kids, The New York Times, November 8, 1988, Tuesday, Late City Final Edition, Section A; Page 16, Column 1; National Desk, 974 words, by John Markoff
9 Nov 1988	BUSINESS TECHNOLOGY; The Computer Jam: How It Came About, The New York Times, November 9, 1988, Wednesday, Late City Final Edition, Section D; Page 10, Column 1; Financial Desk, 1340 words, by John Markoff
9 Nov 1988	Computer Experts Say Virus Carried No Hidden Dangers, The New York Times, November 9, 1988, Wednesday, Late City Final Edition, Section A; Page 18, Column 1; National Desk, 794 words, by John Markoff
11 Nov 1988	U.S. Is Moving to Restrict Access To Facts About Computer Virus, The New York Times, November 11, 1988, Friday, Late City Final Edition, Section A; Page 28, Column 5; National Desk, 795 words, by John Markoff
24 Nov 1988	USSR submits proposal URS/40/5 calling for infrastructure protection obligations for internet arrangements
26 Nov 1988	Cyberpunks Seek Thrills In Computerized Mischief, The New York Times, November 26, 1988, Saturday, Late City Final Edition, Section 1; Page 1, Column 1; Financial Desk, 1705 words, by John Markoff, Special to the New York Times, San Jose, Calif.
28 Nov 1988	Opening of WATTC'88

This Annex is courtesy of John Markoff, who still writes seminal technology articles for the New York *Times*.