Talal Abu-Ghazaleh Domains TAG-Domains

Newsletter

Issue 89 October 2023

IN THIS ISSUE:

Saudi Arabia: Major Change to the Trademark Registration Process

ICANN Publishes Updated Domain Name Marketplace Indicators

DNS Abuse and Redirection: Enough for a New JS Malware to Hide Behind?

Internet Governance in 2023

Saudi Arabia: Major Change to the Trademark Registration Process

RIYADH – The e-filing system of the Saudi Arabia Authority for Intellectual Property (SAIP) no longer allows selecting class headings upon filing trademark applications.

As of November 5, 2023, Saudi Arabia has adopted the 12th Edition of the NICE Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks (NICE Classification).

The applicant for a trademark application can only select specific items of goods/services from the 12th Edition of the NICE Classification using the same wording.

For more information, or inquiries please contact AGIP KSA office at ksa@agip.com

Source:AGIP

ICANN Publishes Updated Domain Name Marketplace Indicators

The Internet Corporation for Assigned Names and Numbers (ICANN) announced the release of an updated indicator schema, taxonomy, and industry metrics, as part of its **Domain Name Marketplace Indicators** initiative.

The initiative presents statistics related to generic top-level domains (gTLDs) and country code top-level domains (ccTLDs) with the aim of fostering greater transparency for reputable information on the evolution of the domain name marketplace.

In recognition of its role as a key source of reputable domain name marketplace indicators, the ICANN organization is formally operationalizing this initiative for annual release, thereby ensuring delivery of updated indicators to the community.

Across four prior releases, between 2019 and 2022, ICANN org progressively expanded its coverage of marketplace indicators to a total of 29 indicators and over a thousand data points. ICANN org has conducted a critical review of the project, assessing indicator use levels alongside the effort required to generate them, with the aim of streamlining future releases and optimizing the efficiency of its work.

An **updated Version 1.1 schema**, which represents the output of this evaluation, is made up of three overarching categories and tracked by a total of 16 indicators relating to dimensions such as registrant choice, registrant domain adoption, service provider marketplace entry and competition, service provider contractual compliance, and industry safeguards. Historical values for indicators previously published, but discontinued under the current schema update, will continue to remain accessible via ICANN's **Open Data Platform.**

"The operationalization and updated schema being made available in this fifth wave of indicator release are a logical next step to focus our efforts in delivering valuable marketplace indicators to the ICANN community," said Theresa Swinehart, Senior Vice President, Global Domains and Strategy. "ICANN will continue to work with the community and its Advisory Panel to evaluate additional enhancements that might be incorporated into this initiative in the future."

Source: ICANN

DNS Abuse and Redirection: Enough for a New JS Malware to Hide Behind?

By WhoisXML API

DNS abuse combined with redirection seems to be gaining popularity as a stealth mechanism. We've just seen Decoy Dog employ the same tactic. More recently, a still-unnamed JavaScript (JS) malware has been wreaking havoc among WordPress site owners by abusing Google Public DNS to redirect victims to tech support scam sites.

Sucuri published an in-depth analysis of the JS malware where it named 30 domains and five IP addresses as indicators of compromise (IoCs). Our research team then sought to find other related threat artifacts through an IoC expansion analysis. Our DNS deep dive uncovered:

- Two unreported IP addresses to which some domains identified as IoCs resolved
- 330 domains that shared the dedicated IP addresses identified as IoCs and the additional ones we found as hosts, 157 of which turned out to be malicious according to a bulk malware check
- 101 domains that contained some of the strings found among those identified as IoCs

A sample of the additional artifacts obtained from our analysis is available for download from our website.

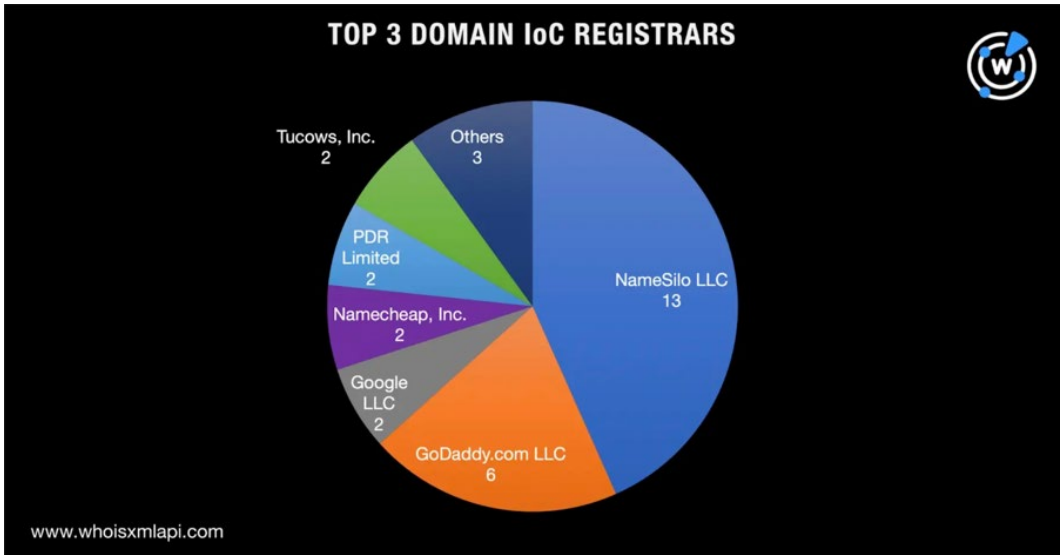
DNS Revelations about the IoCs

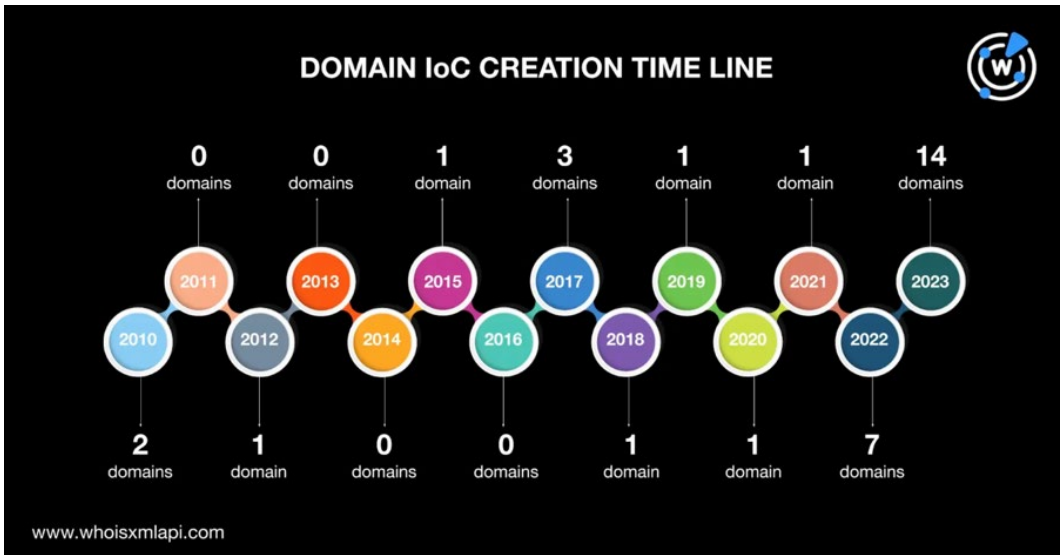
We began our analysis by looking more closely at the IoCs that Sucuri already published.

First, we subjected the 30 domains identified as IoCs to a bulk WHOIS lookup that led to these discoveries:

- The domains were administered by 10 registrars topped by NameSilo LLC in first place (13 IoCs). GoDaddy.com LLC took the second spot with six domains. Google LLC; Namecheap, Inc.; PDR Limited; and Tucows, Inc. shared third place with two IoCs each. The remaining three domains were spread across three registrars.

The IoCs were registered between 2010 and 2023. Further scrutiny revealed that a majority (14 domains) were created just this year, and since another seven IoCs were created in 2022, it's possible that the threat actors favored using newly registered domains (NRDs) in their campaigns.





The majority of the domains (20 IoCs) were registered in the U.S. Two each were registered in Canada, Iceland, and the U.K. Finally, one each was registered in Brazil, Poland, and Vietnam. One domain didn't have a publicly viewable registrant country.

Next, we subjected the five IP addresses identified as IoCs to a bulk IP geolocation lookup that led to these findings:

- Each IP address traced back to a different country—China, Finland, Germany, the U.K., and Russia. The U.K. was the only one that also appeared on the list of registrant countries.
- Two of the IoCs were administered by OVH while the remaining three were spread across AS5398 SA, Hetzner Online GmbH, and Kisara LLC.

New DNS Discoveries

Our bulk WHOIS lookup earlier also revealed that three of the domains identified as IoCs had public registrant email addresses. Through reverse WHOIS pivoting, we found that two of them were used to register two domains that weren't part of Sucruri's list. The first domain, agenciafleek[.]com led to an error page and shared IoC ojosclear[.]com's registrant email address. The second, suffolktrackofficials[.]org, meanwhile, was unreachable at the time of writing but shared IoC look-alike suffolktrackofficials[.]com's registrant email address.

Next, we performed DNS lookups for the 30 domains identified as IoCs and found two IP address resolutions not on the current IoC list. While both 165[.]232[.]94[.]190 and 192[.]124[.]180[.]195 originated from the Netherlands, they had different Internet service providers (ISPs). 165[.]232[.]94[.]190 was under DigitalOcean, LLC management while 192[.]124[.]180[.]195 fell under Teknology SA's purview.

We then subjected the seven IP addresses (five IoCs and two newly discovered artifacts) to reverse IP lookups, which revealed that five of them were seemingly dedicated hosts. They were shared by 330 other domains that weren't part of the existing IoC list. A bulk malware check showed that nearly half of them (157 to be exact) were classified as malicious.

As the last step, we used Domains & Subdomains Discovery to determine if other domain names containing some of the strings present in the 30 domains identified as IoCs were present in the DNS. We found that 11 strings in some of the IoCs also appeared in 101 other domain names. These strings were:

- bonuspremium.
- datingdudes.
- hitjackpot.
- ntertane.
- premiumwin.
- prizeforall.
- profitmagnet.
- suffolktrackofficials.
- sweetsbonus.
- tracker-cloud.
- wantafile.

While none of the 101 string-connected domains have been dubbed malicious to date, some did bear other similarities with the IoCs, such as:

- 14% of the potentially related artifacts shared four of the IoCs' registrars.
- 20% of the similar-looking domains shared some of the IoCs' creation years.
- One of the potentially related artifacts shared one IoC's registrant name.
- 17% of the similar-looking domains shared three of the IoCs' registrant countries.

Our deep dive found hundreds of malicious domains that shared the IoCs' dedicated IP hosts. As threat actors behind the JS malware intend to hide behind traffic redirection in the DNS, those breadcrumbs could help further study and understand the technique.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.

Source: Domain Incite

Internet Governance in 2023

By Geoff Huston

It's been an interesting couple of weeks for me, in mid-October 2023. I presented in a couple of panels at the 18th Internet Governance Forum meeting, held in Kyoto, Japan, and I also listened in to a couple of sessions in their packed agenda. The following week, I followed the presentations at NANOG 89, the meeting of the North American Network Operator's Group, and listened to a presentation by John Curran, the President and CEO of ARIN, where he gave his impressions of the current state of Internet Governance.

There was a time, some decades ago now, when the Internet was seen as a novel space, unpopulated with the adornments of the physical world. Inhabitants of this new Cyberspace felt that they could define their own terms of engagement, equipped with an eloquent declaration of Independence of Cyberspace.

When the Internet outgrew its academic and research roots and gained some prominence and momentum in the broader telecommunications environment, it found itself to be in opposition to many of the established practices of international telecommunications arrangements and even in opposition to the principles that lie behind these arrangements. For many years, public sector policymakers were being lectured that the Internet was "special," and for any nation to consider applying the same mechanisms of national telecommunications and domestic trade regulations to the Internet may not wreck the entire Internet, but they would surely isolate the nation from realizing the future bounties of this new digital age!

Within this broad category was the notion that conventional means of conducting trade in services did not apply to the Internet. While an early mantra of "The Internet must be free" quickly foundered when it encountered the pragmatic realities of having to pay the bills, the next mantra of "Don't tax the Internet" gathered significant momentum. What was meant here was an admonition to governments not to attempt to unduly constrain the flow of data, as such actions would imperil the future value of the Internet and throttle its future from the outset.

But while the Internet might have been "special" in the 1990s, such a characterization was unsustainable in the longer term. In 2003 and 2005, the United Nations hosted the two-part World Summit on the Information Society (WSIS). It was clear by the time of the millennium that the previous regime of national telephone operators and the treaties that governed the international aspects of this global service were rapidly becoming side-lined if they had not been side-lined already. The Internet was sweeping all before it, and each time it engaged with another sector, it appeared to come out of the encounter as a clear victor. The Internet might still be "special," but by the millennium, it was recognized that it was not always special in a good way for everybody!

This WSIS summit was in the context of the emergence of the so-called information society and a recognition of a widening "digital divide" where richer nations were in an obvious position to exploit the possibilities that opened with the combination of abundant computation and communications services and thereby amass further wealth, while poorer nations yet again found themselves on the exploited side of this divide. Far from being a tool to help equalize the inequities in our world by allowing all to access information, education and open global markets for their services, the Internet appeared to be yet another tool to further emphasize and widen this divide between rich and poor.

The United States was a focal point in these discussions. At the time, the Internet was still strongly associated with the United States, and the US had spent much of the previous decade both promoting its benefits and profiting from the global revenues flowing into US companies that represented the vanguard of the Internet. This promotion of the Internet and the free flow of information was certainly not without elements of self-interest on the part of the US, as it appeared that the interests of the new corporate behemoths of the Internet and the geo-political and geo-economic aspirations of the US appeared to have much in common.

However, it's often difficult to tackle the larger picture in these large-scale international forums such as these WSIS meetings, so it was unsurprising to see attention turn to the individual elements that were contained within this picture. One of these elements that became a topic of discussion in its own right was the status of the body that oversaw the Internet's protocol parameters, including the names and IP addresses that are used as part of the central core of the Internet. This function, the Internet Assigned Numbers Authority (IANA), was originally part of the US Defence Advanced Research Project Agency's funded activities. After a few more changes within the US Government's agency landscape, the responsibility for this function had been shifted to a self-funded mode operated by a private sector entity, ICANN, with some level of US Government oversight remaining in place. This ongoing US role was variously portrayed as a control or as a safeguarding measure. Irrespective of the nature of the motivation, the result was that the National Telecommunications and Information Administration, part of the US Department of Commerce, oversaw a contract between the US government and ICANN regarding the operation of the IANA function.

At times, perceptions matter, and the lingering perception here was that the Internet was still seen to be essentially under the control of a single sovereign state, namely the US government.

This unique US role was always going to be a problem for other nations. The international telephone and postal networks were governed by international treaty instruments that had been in place for more than a century. To have a single nation-state positioned at the apex of this global Internet structure was, to say the least, controversial. Naturally, this was a major topic in 2003 at the first WSIS gathering. The UN Secretary-General at the time, Kofi Annan, convened a Working Group on Internet Governance (WGIG), a grand title that either conflated this topic to an even greater level of prominence or appropriately stated its central importance to the entire set of concerns with the structure of the Internet at the time. Again, opinions vary here. There was no clear consensus coming out of this WGIG activity, and the 2005 WSIS gathering could not reach any form of agreement on this matter.

During the WSIS process, the US apparently refused to consider any changes to its pivotal role in the management of the Internet's protocol parameters and had convinced a number of other national delegations to support their stance based on the argument that the available alternatives would return the Internet to the same institutionalized graft and corruption sanctioned by the International Telecommunications Union (ITU) that had bedeviled the international telephone financial settlements.

The WSIS summit eventually agreed on a compromise approach that deferred any determination on this matter and instead decided to convene a series of meetings on the underlying policy principles relating to Internet Governance. Hence, we saw the inauguration of a series of Internet Governance Forum (IGF) meetings. These forums were intended to be non-decisional forums for all stakeholders to debate the issues. Originally intended to be convened for a period of five years, culminating in the fifth IGF meeting in Vilnius, Lithuania, in 2010, it has continued with further extensions of its mandate, and the eighteenth IGF will take place in Kyoto in October 2023.

The early days of the IGF were dominated by the question of the need for some form of international regulatory body for the Internet. Many countries voiced the view that the global communications system should not be operated under the aegis of a single national entity, and the best way to coordinate the actions of various national actors was within a framework defined by an international communications treaty organization, and coincidentally there was such a body with a venerable international pedigree, namely the ITU. The US and a set of sympathetic national delegations were having none of this. AT&T had been very successful in selling the proposition in Washington that the financial accounting structures adoptions by the ITU to balance cost and revenues in supporting international telephony amounted to institutionalised financial extortion, where the victim was the US and AT&T in particular. The US was determined not to allow the Internet to be abused in a similar manner. The US argued that the Internet was a poster child for the flexibility and efficiency of the private sector and that the private sector should exercise self-governance. If the carriage of the provision of services on the Internet is a market-driven outcome, then what is the role of government intervention?

The Internet can be regarded as an open marketplace, where the operators of network services competed for revenue from its users, focusing the attention of network service providers on the issues of quality, relevance, and affordability in their efforts to raise revenue from users. As a backstop, the interests of its users are protected by conventional forms of national market oversight, with provisions for regulatory intervention to counter instances of market distortions and abuse. This essentially economically purist form of market-based disciplines working through competitive pressures to act as the internet's governance framework has offered us a mixed collection of outcomes. The impetus of Moore's Law acting on the underlying currency of computational capability was always going to be challenging. When the unit cost of computation and storage halves every two to three years, and the cost of carriage services is subject to a similar decline, it would always be challenging for the public sector to move with a degree of speed and agility to match the technology-induces changes in the digital environment. The private sector faced similar issues, and their response was directed to contain the levels of disruptive pressure brought about by such an intense level of technical disruption through extensive aggregation within the supply side of the market. The incumbents sought to secure their position and control the levels of disruptive pressure by buying out any emerging future forms of competitive disruption before they attained sufficient market presence to threaten the position of incumbents.

This rapid and large-scale aggregation within the Internet and computing industry had three major outcomes. Firstly, the process of aggregation has resulted in a handful of global digital behemoths that completely dominate the space. Their sheer size and ability to sustain a relationship with every Internet user far exceeds the capability of the various national and regional public sectors, which places negotiations between these digital giants and such public sector regulators on an extremely unequal footing. Secondly, the massive expansion of digital services into all parts of society has created a level of societal dependence on digital infrastructure that has now reached the point of critical dependence for modern society. The third factor arises from the speed of this expansion. The technologies that we rely on are by no means robust. Indeed, they are highly vulnerable and certainly not self-healing when damaged. There is a continual stream of reports of various forms of malicious and accidental disruption that have far-reaching impacts on the normal functioning of our world, from financial fraud infrastructure disruption all the way to interference in domestic elections.

None of these outcomes provide governments with any cause for complacency that this digital transformation is proceeding in a well-ordered and managed manner. Not only are we vulnerable to malicious attacks on the supply chains for food and services attacks on our infrastructure, including traffic control network, water storage and reticulation and power generation, but now we are having a crisis in confidence over the very nature of truth. The capability of generative language systems to provide entirely plausible untruths, coupled with the enthusiasm on the part of these digital

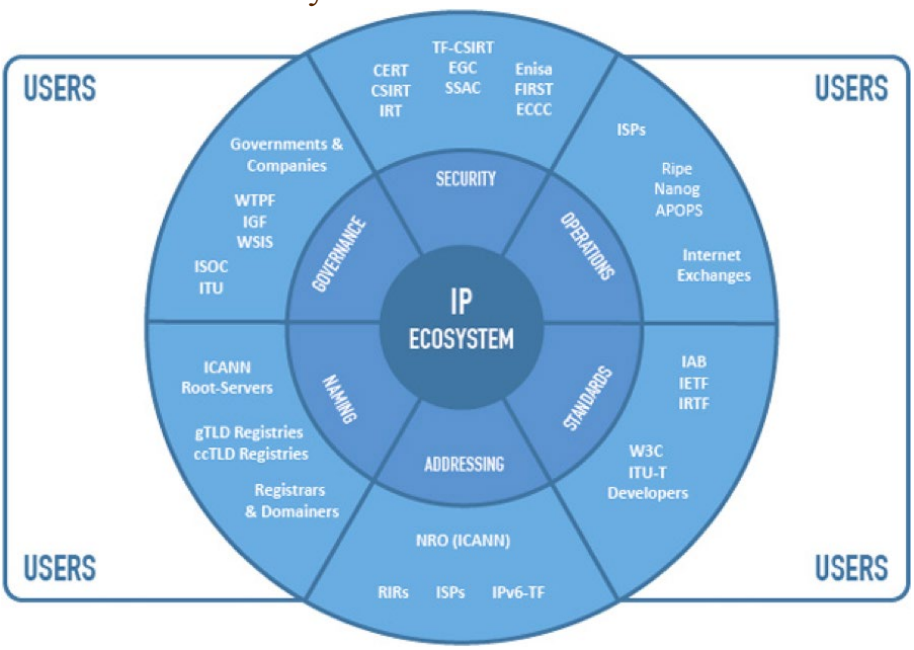
behemoths to embrace such systems, should make all of us, including our public sector, extremely uneasy.

When we consider the topic of "Internet governance," it is this context that should be used for this consideration.

Internet Coordination and Internet Governance

Despite appearances to the opposite, the Internet is not an unconstrained free-for-all. The network is constructed upon a foundation of coordination to sustain a common foundation of names or endpoint addresses, of protocol specifications and, of course, common technical specifications. It is only through a common adherence to these coordination outcomes and suppliers of digital products ensure that their products will interoperate with the rest of the network.

This coordination cannot be undertaken as a set of bilateral arrangements but has to be undertaken as a multi-lateral arrangement that is applied to all. Over many decades, this process has evolved into a collection of open discussions leading to the adoption by consensus of a common framework. In the Internet context, this is termed the "Multi-stakeholder Model" and is visible in the mode of operation of the domain name sector supported by ICANN, in the stewardship of the address system with the operation of the Regional Internet Registries. And development and maintenance of technical standards undertaken by the Internet Engineering Task Force. Similar open processes are used in operational bodies, such as the various Network Operational Groups that operate at both regional and national levels. By developing these common coordinated frameworks in an open consultative fashion using consensus rather than imposed direction, the intention is to arrive at outcomes that are acceptable to all stakeholders. As shown in Figure 1, the scope of these multi-stakeholder coordination efforts encompass a diversity of activity domain within the broader Internet ecosystem.



Can we reframe Internet Governance as Multi-Stakeholder Coordination and just call it all done? Not so fast! There is a definition of Internet Governance from almost two decades ago that I feel is still apposite today. From the World Summit on the Information Society (WSIS) Tunis Agenda convened on the 18th of November 2005, there is the following: "A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."

In particular, the respective role of government in this context includes the definition of commonly acceptable codes of conduct for individuals and institutions for society the enactment of laws and regulations that conform to such codes of conduct. It also includes the exclusive use of force to compel adherence to these laws. It also upholds a concept of the management of public resources for the common good. Government roles typically include national defense, which in recent times has expanded from the traditional military role that defends physical assets to the area of protection of digital assets and defense against various forms of digital threats. In the same vein, the governmental role of the provision of public communication services, where the postal and telephone system was operated as a public sector undertaking, has been expanded to include digital services using the Internet. These internet services are not typically a server operated by a public sector agency but are operated by private sector entities within a regulatory framework that is usually intended to ensure that Internet services provided by these private sector operators are accessible, functional and affordable. The government's economic role, which was traditionally associated with oversight of the national currency and the operation of national financial institutions that stabilize the national economy, now extends to e-commerce and the digital economy. Governments also have a role in maintaining a safe and orderly society, ensuring the rule of law and the protection of individual rights. In the context of the Internet, this includes measures to protect citizens and businesses from cybercrime, and empowering law enforcement to operate effectively in the digital realm. Governments need to define individual rights to privacy and freedom of expression on the Internet within the context of societal norms that apply in other contexts. Safety also includes the regulation of content and services online to protect minors and others from inappropriate content and harmful forms of abusive conduct. That's a big agenda, and it's complicated by the observation that geographical borders do not have a clear counterpart in the digital environment and the ability of one national community to undertake that governmental roles may well be impacted by the positions being take in other realms.

An Internet Governance Scorecard
So, how are we doing so far?
In a word, “badly”.
The online world is replete with all forms of bad behaviors. Vulnerabilities, once exposed, are invariably exploited. Individual businesses and public institutions have fallen as victim to various forms of cyber-attack. Our efforts to respond to such incidents are not exactly reassuring, as the frequency and severity of such incidents appear to completely overwhelm the resources we can amass in response to such incidents.

It appears that we are constructing ever more complex systems whose inner workings are dimly understood, if at all. The result is that we field partially tested systems that most likely contain vulnerabilities and leave it to users to be the field testers. Yes, these are complex systems, and comprehensive testing of all potential scenarios is prohibitively challenging, but in many cases, it appears that the pre-release checks and tests are more perfunctory than substantive. It seems that much of the supply side is still working to Mark Zuckerberg’s directive to “Move fast and break things!” No matter how good our incident response framework may be, if the supplied materials are faulty in the first place, this situation is never going to get any better.

But it gets worse. The rapacious silicon chip manufacturing industry keeps on motivating ever higher volumes of consumption of chips, and we are embedding functionality into billions of consumer devices that are sold as commodity goods. The cyber-defensive capability of these unmanaged devices is non-existent, and the consequences of co-opting such devices into a zombie army are worrisome. We just don’t have answers here.

Our societies are now critically dependent on the continuous operation of the Internet and equally dependent on the ability of the devices that use the network to be impervious to efforts to corrupt their operation. In the face of continual incidents that demonstrate the folly of such levels of dependence, we simply increase court collective dependence as we push more functions into the digital world in the name of economies of operation.

The impacts of these failings in the robustness, safety and security of the digital ecosystem have concerning ramifications. There is a considerable economic cost of various forms of disruption to the online environment.

The consulting firm Deloitte published a study in 2016 on the economic impact of disruptions to Internet connectivity

That report estimated that the per-day impact of a temporary shutdown would be, on average, $23.6 million per 10 million population in a highly connected economy. Some seven years later, it's likely that one could increase this estimated cost metric by an order of magnitude!

There are major concerns in the area of national security and the protection of national infrastructure. Attacks on public services, be it health providers, online government service provision, or even online census activities, have been a continuing illustration of the level of hostility in today's Internet.

So, while it may have been a bold, even courageous, decision some years ago to deregulate the national telecommunications sector and open the operator of this public service to competition from the private sector, it would be a foolhardy government to claim that they can persist with a laissez-faire attitude and believe that market forces will provide remedies for this current situation. The auto industry is a good case in point that regulatory intervention was required to focus that industry on human safety.

Moving Forward…

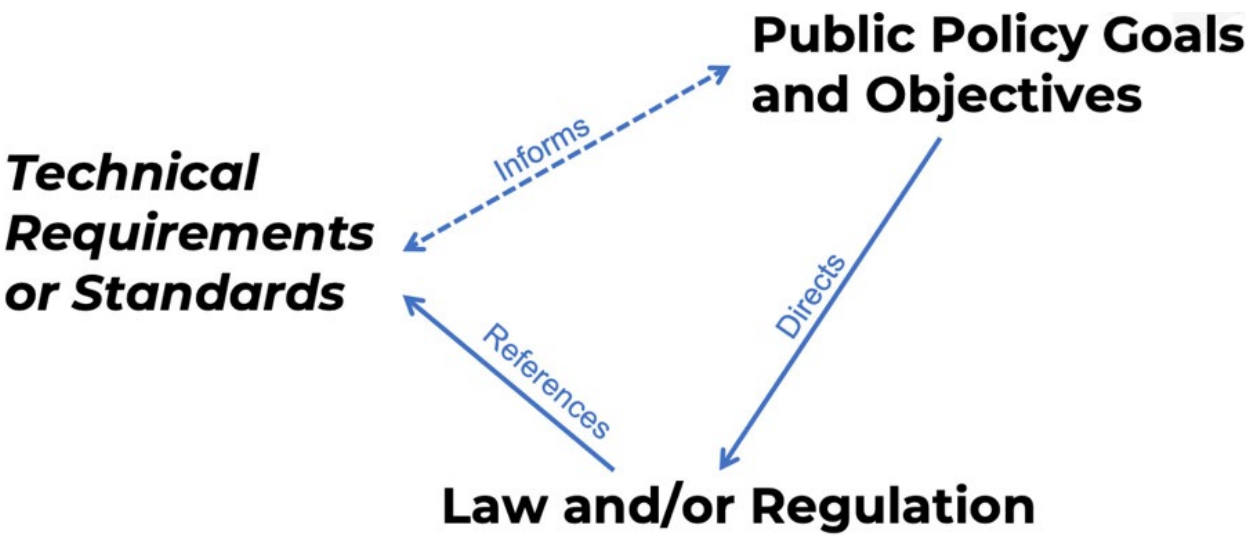
How can national governments fulfill their roles and duties in fostering an Internet that is safer for users, protects the integrity of online services, and protects elements of national infrastructure while allowing the national economy to benefit from the efficiency in the digital delivery of goods and services? How can a national environment counter the situation that its critical elements of digital infrastructure are operated by foreign entities who owe no accountability or obedience to national laws and regulatory measures without encountering punitive additional costs? How can a national community realize the economies of global scale without passing control of their national digital infrastructure to global operators?

The next steps for governments in the overall governance of this digital space (or "the Internet," if you prefer) are clearly posted in their legislative and regulatory actions. The EU has moved to try and correct the overt abuse of personal data by large digital enterprises with the General Data Protection Regulation (GDPR), the more recent Digital Services Act and the Digital Markets Act. There are measures relating to content moderation, protection of minors and personal data privacy. If digital platforms believed that the profile information that they gleaned from providing services to individuals was their private property to do with as they wanted to further their commercial objectives, then these legislative measures place a curb on such beliefs.

Over the years, the public sector has become more confident in its own capabilities and far less tolerant of the claim that any measures to curb the behaviors of the digital giants would destroy the entire value of the digital economy. Given that many of these digital giants have their corporate domicile in the US, it's unsurprising that the EU has felt that its citizens are the exploited party here and has been more inclined to take such regulatory measures that impact the commercial practices of these entities.

The situation in the US has manifested itself in perhaps more disturbing ways, where there is a visible societal gap between a so-called "digital elite" and an estranged class who feel that their social position and prospects are being irrevocably eroded. The result is a national democratic structure that is undergoing a traumatic crisis of confidence. As a consequence, there is less of a legislative appetite to enact such measures due to these deep divisions that extend all the way into the legislative bodies.

In consideration of this governance space so far, we have noted the public interest role of a public communications service and the role of governments in creating requirements of the operators in this space that are intended to curb the behaviors of the operators of this service in order to meet the associated public policy goals. What we've omitted so far here is the role of technical standards that define the profiles of technology elements and operational practices that are intended to ensure that the diverse collection of operators and their various supply channels can generate services that interoperate with the offerings from other service providers. The cohesion of the network as a compound entity depends on the common reliance on these standard specifications and profiles. The implication of this observation of common reliance on technical standards and operational profiles is that the bodies that generate these standards are themselves an integral part of the overall landscape of Internet Governance.



The technology specifications that are developed by the standards bodies are certainly informed by the goals and objectives of public expectations about the technology process. For example, the public concerns over the use of digital surveillance mechanisms by US agencies, as revealed in the Snowden documents of 2013, motivated as reaction in the Internet Engineering Task Force (IETF) (RFC 7258, " Pervasive Monitoring Is an Attack", May 2014) that led to the adoption of strong privacy measures in many IETF-specified protocols thereafter. At the same tome, the capabilities described in these technology specifications inform the public policy conversation, not only in defining the scope of the conversation but also in illustrating feasible objectives for the public policy process.

In a recent presentation to the North American Network Operators Group (NANOG), ARIN's John Curran made the point that it would be helpful if there were a commonly understood set of roles for governments and the Internet technical community within the Internet Governance model. The globally connected nature of the Internet requires that the technical specifications and standard operational practices must also be global in scope, and to achieve common acceptance of such standards they need to be developed within a consensus-based multi-stakeholder process. The credibility and acceptance of such standards is not by mandate but by common recognition of their inherent value as a means of seamless interoperation in an interconnected environment.

While it is not the role of governments to also develop such technical standards, it is appropriate for governments to be informed by and reference such standards in regulatory measures as an expression of common behaviors that are consistent with the regulatory intent. John observed that the role of governments lies in the implementation of public policy objectives through the development of appropriate national (or regional) law and regulation and that, with respect to the Internet in particular, such regulation should reference the global technical standards and practices developed by the Internet technical community as appropriate.

There is no doubt that these days, governments feel a pressing need to engage in the Internet Governance conversation and be seen to take visible steps to mitigate the threats that are posed by a highly toxic digital environment. The temptation to take unilateral steps and mandate behaviors through legislation is invariably related to the perceived severity and urgency of the threat.

I'm not sure that the cyber threat model has escalated from a series of "incidents" to a full-blown "disaster", and I'd like to think that we still have some time before we reach that acute level of digital clamity. I'd like to think that there is still time for better engagement between the public policy environment and the technical community, particularly in the realm of technical standards and the specification of operational practices.

However, the barriers to such outcomes are considerable. Anyone who has attended IGF meetings must be aware of the dramatic difference in vocabulary between these communities. There is a distinct impression of frustration from many technical participants that the technical messages need to be simplified and sliced into extremely small portions. Even then, it often feels as if the major thrust of the technical message has somehow been lost in translation. I'm also sure that many folks with a background in public policy see the technical conversations in IGF forums as being deliberately shrouded in obscure jargon to make the technical considerations largely impenetrable to non-technical folk.

However, there are hopeful signs in the technical space. A frequently quoted program in the routing security space is the MANRS program, which is essentially a common code of conduct for operators of networks who have to publicly commit to adopting practices that support the robustness and security of the routing system. A similar program in the namespace, KINDNS, provides a similar code for operators of the Internet's naming infrastructure. Such initiatives provide a middle path of describing the intent of the technical activities in terms that are intended to resonate with the concerns of the public policy space.

I'd like to think that the principles of an open and accessible technology foundation are an intrinsic component of open, accessible and healthy societies. I'd like to think that the principles of accessibility, transparency and diversity that are part of the mode of operation of the multi-stakeholder process are valuable principles and should ensure a healthy and robust debate on the various topics of Internet Governance. I believe that the IGF has been of assistance to the increasing level of shared understanding of the Internet, in both its strengths and its weaknesses. I suspect that Internet Governance will become irrelevant only when we let it become so. Like any open, cooperative effort, it requires continual care and attention if it is to continue to flourish.

But there is another side to this issue. We are embarking on changes in our society that are as dramatic and even as traumatic as the Industrial Revolution or the rise of the printing press in Western European history. Such revolutions leave a path of social dislocation and uncertainty in their wake, and this digital revolution is no exception. It is perhaps unsurprising that nation-states tend to be more assertive in such situations as they try and mitigate some of the worst excesses of such social disruptions. One side-effect of this increasing nationalistic stance is that the various international efforts, both regional and global, tend to be regarded with increasing levels of distrust from these national regimes. In times of uncertainty and stress, nations naturally try to raise the drawbridge and attempt to insulate themselves from such disruptions by asserting greater levels of control within their own national realm.

The refinement of the steam engine certainly triggered the Industrial Revolution, but the social revolution was far larger in scope than the invention of a simple mechanical device. In a similar line of thought, maybe it's not the Internet or its governance that lies at the heart of many of today's issues. Maybe it's the broader issues of our enthusiastic adoption of computing and communications that form a propulsive force for disruption in today's world, and the destructive side effects that invariably accompany such disruption.

Maybe it would not be a bad thing after all if the inexorable pressures of Moore's Law down in the silicon chip engine room were to come to a graceful halt in the near future! We need some time to catch our breath and look at the world we are building. Are we building a world that is fairer and better balanced? Or is this just another round to division and exploitation where the fault lines of division now lie between the techno-elite and everyone else? If data is the new currency of digital wealth, then how can we counter our data being stolen, aggregated and ruthlessly exploited by today's data behemoths?

There sure is a lot to do out there!

Source: Circle ID

Please feel free to contact us at:
info@tag-domains.com
Tel.: +962 6 5100 900 ext. 2743
Fax: +962 6 5100 901

TAGTech PRODUCTS

FLIP

- Intel Core i5 8th Generation
- 8 GB RAM DDR4
- 256 GB SSD

PRO

- Intel® Core i7 10th Generation 1065G7
- 8 GB RAM DDR4
- 128 GB SSD + 512 GB SSD

UNI C

- Intel Celeron N4100
- 4 GB LPDDR3
- 256GB SSD + 64GB EMMC

EDU

- Intel® Core i3 10th Generation 1005G1
- 4 GB RAM DDR4
- 128 GB SSD

PLUS I

- Intel® Core i7 10th Generation 10510U
- 8 GB RAM DDR4
- 128 GB SSD + 1 TB HDD

PLUS II

- Intel® Core i7 10th Generation 10510U
- 8 GB RAM DDR4
- 128 GB SSD + 512GB HDD

PLUS III 7022

New

- Intel® Core™ i7 1255U
- 8 GB RAM DDR4
- 256 GB SSD + 1 TB HDD
- Intel® Iris® Xe Graphics
- 4500 mAh
- AX (wifi 6) BT 5.1

PLUS III 5022

New

- Intel® Core™ i5 1235U
- 8 GB RAM DDR4
- 256 GB SSD + 1 TB HDD
- Intel® Iris® Xe Graphics
- 5000 mAh
- AC WIFI BT 4.2

TAG-TAB KIDS II

- Spreadtrum SC7731E Quad-core
- 2 GB
- 32 GB

TAG-TAB III

- MediaTek MTK 8788 octa-core
- 8 GB
- 128 GB

TAG-PHONE Special

- Front: 16 MP
- Rear: 20 MP
- 6 GB
- 128 GB

TAG-DC

- Spreadtrum SC9863 Octa-core
- 4 GB
- 64 GB

TAG-PHONE Plus

- Front: 8 MP
- Rear: 16 MP
- 4 GB
- 128 GB

TAG-PHONE Advanced

- Front: 16 MP
- Rear: 16 MP
- 6 GB
- 128 GB

TAGTech.Global Building 7, Abdel Rahim Al-Waked Street, Shmeisani, Amman, Jordan
TAGUCI Building104 Mecca Street, Um-Uthaina, Amman, Jordan
+962 65100 250 info@tagtech.global For More Information: www.tagtech.global