Cyberpeace: Why Internet Governance Matters for Global Peace and Stability

Dr Paul Antony White
Politics and International Relations
Leeds Beckett University

Abstract

While the governance of the Internet is often assumed to be merely a technical matter, it is actually a fiercely contested political arena, in which institutional arrangements are still being shaped. This paper aims to demonstrate how, and why, the politics surrounding Internet governance are of significance for international peace and stability. The Internet has great potential as a facilitator of the peacebuilding process, but it can also be used as a tool of oppression, a channel for disinformation and propaganda, and even as a means of waging war. The institutions that are built around Internet governance will determine in whose hands ultimate control of the network will lie, and will ultimately decide whether the Internet is to be a vehicle of human liberation and peacebuilding, or a tool of oppression and conflict. To accomplish the latter, there is a need to move away from traditional state-based assumptions around global governance and security.

Introduction

This article explores the issue-area of Internet governance in terms of its implications for global peace and stability. While matters of Internet governance are often dismissed as ‘low politics’ and mere ‘technical co-ordination,’ control over the network is in fact a matter of considerable interest and importance both to governments and to nonstate actors. As such, the issue-area has become increasingly politicised since the turn of the millennium. Some of the key concerns relate to security and the perceived new threats, as well as opportunities, created by the Internet’s emergence as a critical economic and social infrastructure. As a new and dynamic medium for the transmission and dissemination of political ideas, the network can be a platform for peace education and a medium for peacebuilding dialogue across lines of conflict. However, it can also be a channel for messages of hate and warlike propaganda, and a tool of radicalization. More than this, there is very real potential for the network itself to become a domain of conflict. Increasingly sophisticated cyberwarfare techniques and cyberweapons are being rapidly developed, and in some cases deployed, both by states and nonstate actors. Cyberwarfare has the potential to produce very real consequences in the real, physical world.

Not only could cyberattacks directly cause large scale disruption and even significant loss of life, they could also bring about political destabilization and escalation that could lead to conventional kinetic warfare. These dangers should not be underestimated or taken lightly.

To date, governments have tended to approach cyberconflict in terms of established thinking about 'national security.' These approaches, which are ultimately based on 'realist' conceptualizations of security, begin from 'statist' assumptions. Essentially, they frame cyberwarfare in territorial terms. The goals are assumed to be the defense of national infrastructure (virtual 'territory'), and acquisition of offensive capabilities to attack the virtual 'territory' of a clearly defined opponent. Cyberwarfare capabilities are treated as instruments of power, in a fundamentally similar manner to military capabilities. Familiar concepts and models such as the notion of defense and offense, arms races, and balances of power are assumed to apply in cyberspace. Such thinking is not only problematic, but is demonstrably dangerous. Territorial approaches to Internet governance may threaten the medium's peacebuilding potential. The article will demonstrate how the Internet can be used positively in the cause of peacebuilding, and explain why that potential may be threatened by governmental attempts to extend their control over the network.

An analysis of the Internet's basic nature, consideration of the fundamental requirements for Internet governance, and reflection on its evolution to date, shows that the best prospects for dealing with these issues lie in reaffirmation and reinforcement of the non-governmental multistakeholder model of Internet governance. Specifically, the development of new and strengthened multistakeholder institutions at the global level will be recommended. The notion of nonstate governance is, of course, not new in IR scholarship or indeed in practice, and in recent decades nongovernmental governance arrangements have developed in a wide range of global issue-areas. However, the idea of applying nonstate governance approaches to matters of 'national security' (as perceived by governments) may be less readily accepted. The evidence suggests that multistakeholderism, rather than 'statism,' is key to securing an 'Internet for peace.'

Internet governance: A brief overview

The Internet can be described as a globe-spanning collection of interconnected networks (hence the term ‘inter-net’). Although the Internet has no single owner or oversight body, there is nonetheless a need for a mutually agreed set of common communication standards (‘protocols’), without which universal communication would be impossible. This need for order and uniformity implies a requirement for governance mechanisms. Rather than a single overall governing body, various institutions exercise coordination and control over different aspects of Internet governance, having evolved out of what initially were quite ad-hoc arrangements.

One influential definition of Internet governance is that established by the UN’s Working Group on Internet Governance prior to the 2005 World Summit on the Information Society (WSIS): “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.”[1]
This definition reflects the so-called ‘multistakeholder’ approach to Internet governance; a model based around engagement of multiple ‘stakeholders’—governments, the private sector and civil society.

A detailed account of current Internet governance arrangements is beyond the scope of this study, and a summary of the key dimensions provides a solid basis for the analysis to follow. Yochai Benkler[2] conceptualized Internet governance as being composed of three “layers.” The physical infrastructure layer includes physical hardware, cables and connections. The code or logical layer is software protocols. The content layer is comprised of the information that is transmitted through the network. In practice, the politics of Internet governance is not so neatly separated into these three dimensions. In particular, control of both the physical infrastructure and the software layer can confer the ability to control or restrict the free flow of information. Nonetheless, Benkler’s model is a starting point for understanding some of the main aspects of Internet governance.

In terms of the ‘physical layer,’ the hardware and connections (cables, servers, routers, etc.) that make up the network are controlled by Internet Service Providers. These are mostly private companies, though in some cases they may be state owned or controlled. With regards to standards setting, ITU regulations have some influence at the physical hardware level, though much less so on the ‘logical layer.’ The ‘logical layer’ is comprised of the software standards and protocols that make communication possible, as well as the naming and addressing system that allows resources on the network to be located and communications delivered to the intended recipient. Software standards are largely the remit of the Internet Society (ISOC) and its daughter bodies, the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRTF). ISOC is a non-profit NGO founded in 1992 to provide an organizational umbrella for the Internet standards bodies. It is made up of both organizational and individual members, and membership is open to any individual. Its technical standards bodies, such as the IETF, are made up of volunteers from the technical community, though their work is often funded by their employers or sponsors. Another organization producing software standards relevant to Web technology is the World Wide Web Consortium (W3C), an organization made up of businesses, nonprofit organizations, universities, governmental entities, and individuals. Governance of IP addressing and the Domain Name System (which also falls under the ‘logical layer’) is the remit of the Internet Corporation for Assigned Names and Numbers (ICANN). This is another 'multistakeholder' organization whose major stakeholders include key players in the industry. Many of these are private sector corporations, but there is also some representation for governments and civil society.

With regards to content, there is no overall global regulator. There is some limited intergovernmental agreement on content regulation in the form of the 2001 Convention on Cybercrime. This defines the transmission of certain types of content (mainly material already widely illegal in most countries, such as child pornography) as a criminal offense, and seeks to harmonize national law in these areas as well as facilitate cooperation on enforcement.[3] Other international treaties also have some relevance to Internet content, for example the international intellectual property protection regime. Beyond this, most governments seek to regulate content in some way at national level.

Present governance arrangements evolved as the Internet developed from ARPANET, originally a US military network, later primarily used by academics and researchers prior to commercialization in the 1990s. Despite ARPANET's origins, development of the global network took place largely outside of the oversight of governments and the ITU. In 1998, management of the naming and addressing systems was "privatized" by the Clinton Administration, leading to the creation of ICANN. Other aspects of Internet infrastructure management, such as standards setting, were initially decided on an ad-hoc basis by a small technical community. Later, more formalized institutions evolved out of these early ad-hoc arrangements, leading to the foundation of ISOC and its subsidiary bodies. Over the past two decades, as the Internet has become more commercialized and mission-critical for business, commercial entities and interests have become increasingly important stakeholders in these governance institutions.

From around the turn of the millennium, governments became increasingly interested in Internet governance as they began to identify key 'national' interests in the issue-area. The 2003 / 2005 World Summit on the Information Society (WSIS) has been identified as a key catalyst for this shift and has been described as the formal emergence of the international political dimension of Internet governance.[4] One result of the conference was a declaration of governmental claims to sovereign authority in matters of Internet governance.[5] Proposals for a new global Internet authority based around an 'Inter-Governmental Council,' floated at WSIS with the backing of a number of governments, were defeated largely due to the opposition of the United States.[6] Attempts to extend UN / ITU authority over the Internet at the World Conference on International Telecommunications (WCIT) in 2012 were similarly unsuccessful. Nonetheless, the contest between these two competing visions—governmental vs. multistakeholder approaches—remains the most fundamental division in debates around future Internet governance arrangements. Meanwhile, within existing institutional arrangements, both governments and a range of nongovernmental actors continue to compete in their attempts to extend their influence. The struggle for ultimate control of the Internet is still very much an ongoing process, with implications for the futures of both warfare and peacebuilding.

The nature of the threat

The Internet has created a number of potential challenges to global peace and stability. One such challenge derives from its potential as a conduit for spreading messages of hate and conflict, and warlike propaganda. Militant groups are able to use social media and mobile apps to reach a wider audience than ever before. ISIL, for example, have promoted their message through social media and social networks across the globe. The Internet provides opportunities for radicalisation and recruitment,[7] and can also be used to disseminate practical instructions to terror recruits, such as training materials on how to create and use explosives and carry out attacks, and to gather information about targets.[8] States, too, can use the control and manipulation of information as an instrument of warfare. Russia, for example, has developed information warfare techniques aimed at disrupting a target state's command and control systems as well as influencing public opinion on the opposing side, inducing apprehension and undermining trust in government, and ultimately lowering the will to resist.[9] In Georgia and Ukraine, such Russian campaigns of disinformation have been credited with bending public perceptions in line with the goals of the Russian leadership, producing a loss of trust in the ruling elite and weakening resistance.[10]

The Internet can also be a channel for direct attacks. The term 'cyberwarfare' is now in widespread usage to refer to the use of digital attacks to harm a target entity's computer systems and infrastructure. The attacker and target may be nation-states, or either or both may be nonstate actors. Cyberwarfare could potentially produce highly disruptive, even disastrous consequences in the real, physical world. Economically advanced states have become critically dependent on linked computer networks that control much of their infrastructure, including services such as the power grid, communications, financial transactions, government administration, emergency services coordination, transport infrastructure, and even water supply and sanitation. Actions such as shutting down the power supply, interfering with stock exchanges or deleting bank records could cause very significant disruption and large financial costs to any economy. Cyberattacks could also easily cause loss of life, perhaps on a significant scale, for example through disruption of emergency or medical services, manipulation of air traffic or train control systems signals, or nuclear reactor control systems. Hackers might even be able to target military systems such as communications and missile or drone control systems, although in theory such systems ought to be more secure for the most part compared with civilian infrastructure.

Ultimately, cyberattacks could escalate into armed conflict. A serious digital attack that produced significant destruction or disruption or loss of life might be seen as the equivalent of a physical attack. Under international law, states are permitted to use force to defend themselves against armed attack. A state hit by a cyberattack of sufficient magnitude would arguably be within its rights to strike back using conventional military means. While this has not yet happened, governments appear to take the possibility seriously. For example, in 2014 NATO produced a declaration stating that the impact of cyberattacks ‘could be as harmful to modern societies as a conventional attack’ and that a cyberattack on a NATO member could therefore lead to the invocation of Article 5 of the North Atlantic Treaty.[11] A majority of states now treat cyberwarfare as a component of their national defence strategy. In 2013, the United Nations Institute for Disarmament Research produced a 'Cyber Index' which listed 114 national cybersecurity programmes worldwide, with more than forty-five states operating cybersecurity programs that give some role to the armed forces.[12]

There have already been concrete instances of cyberwarfare being used in practice. The Stuxnet worm, allegedly created as part of a joint US-Israeli effort, disrupted Iranian nuclear facilities in 2010.[13] Russia’s campaigns in Georgia and Ukraine were accompanied by actions such as Distributed Denial of Service (DDoS) attacks against Georgian and Ukrainian government and news media websites, interference with mobile phones belonging to parliamentarians, and the infection of Ukrainian government computers with malicious software capable of extracting sensitive information.[14] The cyber-campaign against Ukraine appears to have continued after 2014.[15] Again, groups other than states are also capable of using such methods of attack. Indeed, the cyber realm represents an area where nonstate actors may be able to develop a credible capability with relative ease.

Clearly, therefore, neither policymakers nor the academic community can afford to ignore these rapidly evolving threats to international peace and stability. Indeed, such developments could potentially cause us to reconsider our very definitions of peace and war. To date, however, governments have typically responded by treating cyberwarfare essentially as an extension of traditional interstate conflict, developing cybersecurity strategies that are conceptually rooted in conventional understandings of interstate power relations.

Cybersecurity and state responses

As Stephen Walt pointed out, IR theory shapes public discourse and policy analysis.[16] Many of the concepts that underpin 'traditional' state responses to matters of security have been drawn from what might broadly be called 'realist' assumptions. These include a conceptualisation of defence and security in territorial terms, in an anarchic world system where states are the predominant actors. The Realist paradigm assumes a basic rationality on the part of these state actors, who are assumed to think strategically about how best to ensure their own survival in the international system. However, these calculations are made under conditions of uncertainty; no state can be sure of the intentions of other states. Each state must therefore work on the assumption that other states pose a threat, and will interpret their actions in that light, taking actions to counter those perceived threats based on the self-help principle. Though alliances of states against a common threat can and do occur, these always represent temporary alliances of convenience and can be expected to break down as and when circumstances change. 'Structural' or 'neorealist' approaches, in particular, emphasise a system structure based on relative power capabilities. ‘Power’ is assumed to be zero-sum game; a relative power gain for one state is always a relative power loss for other states. ‘Power’ is based primarily upon military and economic capabilities (though these capabilities are the tools that lead to power, rather than being synonymous with power).

Latter-day neorealist approaches are often classified into ‘offensive’ and ‘defensive’ models. ‘Offensive’ neorealism, particularly associated with John Mearsheimer,[17] assumes that the international system structure forces states to take an aggressive power maximisation approach. By contrast, ‘defensive’ neorealism, associated with Kenneth Waltz,[18] emphasises security maximisation. The assumption here is that state actors will usually follow a ‘defensive’ set of policies that seek to maintain their own integrity and survival. Most states seek to preserve the status quo, although a few ‘revisionist’ states may seek to change it. From a defensive neorealist standpoint, the balance of power is key to preserving stability. Linked to the balancing strategy is the concept of deterrence, particularly emphasised with regard to the nuclear balance during the Cold War period. However, even a ‘defensive’ security maximisation strategy can potentially have destabilising effects. The concepts of the security dilemma and conflict spiral are based on the notion that actions taken by a state with the intention of increasing its own security, such as strengthening its military or forming alliances, may be seen by other states as threats to their own security, which can cause them to reciprocate.[19] This can result in a ‘spiral’ of reaction and counter-reaction leading to an arms race, increasing tensions, a fluctuating balance of power and increasing instability.[20] Under such conditions, the chances of miscalculation resulting in conflict are heightened.

Policymakers have tended to interpret the cyber threat through such traditional security lenses. Indeed, the very term ‘cyberwarfare’ underlines the perception that digital conflicts are conceptually similar to conventional war. Cybersecurity is generally understood by policymakers using the language of threat to the nation state, and cyberspace itself is understood as being analogous to the physical domains of conventional warfare (land, sea, air and space). Governments are deeply concerned with securing their own ‘territory’ (national networks and infrastructure) against incoming cyberattack. [21] In practice, though, cyberattacks are notoriously difficult to defend against. While certain critical systems such as military networks are likely to be well protected, any computer or device connected to the public Internet could potentially be compromised. Vast areas of infrastructure are thus vulnerable. Furthermore, it is nearly impossible to see or anticipate an incoming attack, and cyberattacks can be carried out almost instantaneously. Since it is far easier for a sophisticated cyberattacker to inflict massive damage on a nation's digital infrastructure than it is to defend against such an attack, it could be concluded that cyberwarfare favours an offensive strategy. Both offensive and defensive realists refer to the idea of 'first strike' capability as a way to end a security dilemma by means of a surprise pre-emptive attack that destroys the enemy's ability to respond. Governments are indeed currently engaged in a race to develop their own offensive cyber capabilities.[22] However, any aspirations to develop a first strike capability in cyberwarfare are likely to be fruitless. It is highly unlikely that even the most devastating cyberoffensive would ensure that the enemy cannot retaliate. Moreover, such retaliation may not be in kind, but instead may involve escalation into conventional warfare.

In reality, neither defensive nor offensive realist security strategies are particularly appropriate or helpful in the context of the Internet. Although the concept of anarchy is certainly applicable to the Internet, conventional 'territorial' conceptualisations of warfare do not map well to cyberspace, where national boundaries are not clearly defined and neither is 'the enemy.' Nor can it be assumed that major threats will always come from other states, when dealing with a domain of conflict where nonstate actors can acquire credible capabilities. Such nonstate actors could physically be located anywhere on the globe – even inside the borders of the state being attacked – and may have no official leaders, or physical meeting places to target. Furthermore, if 'territorial' thinking about security is problematic in cyberspace, the applicability of conventional understandings around national interest, power and power calculations are also called into question.

In conventional realist thinking, state interest lies in the maximisation of capability, which confers the ability to wield power.[23] 'Power' is conventionally defined as the ability to bring about desired outcomes, and / or to exercise influence over other actors. While the capabilities that lead to power are not the same thing as power itself,[24] capabilities are the means by which power may be exerted. This logic may appear to be transferable to cyber-capabilities. Joseph Nye uses the term 'cyber power', which he defines as 'the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain'.[25] It is certainly possible that, under the right circumstances, cyber capabilities may constitute a tool with which to obtain desired outcomes or to influence other actors. However, attempting to do so may produce unpredictable results. Any attempt to make power calculations with regard to cyberspace is likely to be fraught with uncertainty. Whereas states generally have a fairly reliable picture of how their own conventional military capabilities compare to those of other states, they are less likely to possess reliable information about the cyber-capabilities of their potential adversaries. Furthermore, cyber-capabilities can change very rapidly compared to the timescales involved for a conventional military buildup. This means that the 'power balance' in cyberspace is not only difficult to establish, but is also likely to be quite fluid and subject to rapid fluctuation. A 'weak' state in conventional terms might rapidly develop the capabilities to be a great power in cyberspace, as evidenced by the increasing sophistication and efficacy of the North Korean cyber programme.[26] The potential for nonstate actors to develop significant capabilities complicates the situation even further. Thus, any attempt to make rational power calculations is likely to be highly problematic. As a consequence, both 'offensive' power maximization strategies and 'defensive' balance of power strategies are rendered unreliable**.**

As well as uncertainty over each other's capabilities, actors face further uncertainty due to the potential difficulties around attribution of an attack. The possibility of maintaining 'plausible deniability' may tempt actors into attempting a first strike, rendering deterrence strategies useless. There is also a danger that governments may see a cyberstrike as a 'safer,' less risky means of attacking an opponent, again increasing the temptation to use cyberweapons. This could prove to be a miscalculation, however, if the adversary unexpectedly responded with conventional force. This heightened uncertainty and potential for miscalculation makes cyberspace a much more dangerous place to play power games than in the conventional physical world, where actors may be uncertain of each other's intentions but at least are able to make relatively reliable calculations about the balance of power and the likely consequences of their decisions.

Fundamentally, the power balance in cyberspace does not represent the sort of zero-sum game assumed by realists. Due to the uncertainty and potential instability created by the prospect of cyberwar, all states, not just some, experience reduced security. Security in cyberspace is therefore a collective matter across all states and their citizens. This line of thinking might appear to lead to an argument in favor of a multilateral, collective security response as an alternative to 'realist' security strategies. On the face of it, such an argument would appear to have much merit. In the absence of established norms and shared expectations among actors, there is a higher probability of miscalculation and unintended escalation. A multilateral convention on cyberwarfare might lead to the establishment of mutually understood rules and norms that could reduce the potential for such miscalculation. Such a convention could work out some 'rules of war' in cyberspace and help to define some basic common understandings, such as what constitutes a cyberattack and what an appropriate response might be. Consideration might even be given to creating a nonaggression pact for cyberspace or a cyber-arms control treaty that would outlaw certain types of cyber-weapons. However, while such an approach might appear at first glance to offer a route forward, there would be practical difficulties resulting from the nature of cyberweapons and cyberwarfare. Terms such as 'cyberweapon' and 'malicious code' are difficult to precisely define, and there would also be issues in verifying compliance. It would be far more difficult to inspect for cyberweapons than, for example, nuclear or chemical capabilities, given that such weapons could be easily hidden on small, portable media. Cyberweapons, once created, are also easily replicated and proliferated at minimal cost. Furthermore, any norms around cyberwarfare established by interstate agreement would not necessarily be respected by nonstate actors.

In summary, attempting to extend the traditional interstate power game to cyberspace is inappropriate and indeed dangerous. Multilateral initiatives among states might help establish some norms around cyberwarfare and thus create a little more stability, but the collective security approach can only take us so far. Fundamentally, security in cyberspace needs to be conceptualised in broader terms than the traditional interstate approach. Unfortunately, governments have not yet been willing to consider this. In continuing to conceptualize cyberspace in terms of 'national interests,' they actually risk undermining their own security and that of other states. Their attempts to regulate and secure their own 'national' networks may also be counterproductive in another respect, in that such actions may actively undermine the Internet's potential as a positive peacebuilding medium. The next sections will expand upon this point.

The Internet as a positive force for peace

While previous sections have examined the threats that the Internet might pose to international peace and stability, it should also be emphasised that the network has great potential as a peacebuilding medium. Indeed, in 2010, the Internet was nominated for a Nobel Peace Prize for advancing 'dialogue, debate and consensus'. The nomination was sponsored by *Wired* magazine (Italian edition). Riccardo Luna, the magazine's Editor-in-Chief, commented that "The internet can be considered the first weapon of mass construction, which we can deploy to destroy hate and conflict and to propagate peace and democracy."[27] This statement sums up the Internet's potential as a tool of conflict transformation and resolution.

Arguably, the shifting of political and social movements to the online realm may sometimes offer a means of avoiding physical conflict altogether, by providing an easy-to access mass medium where grievances can be aired and policy objectives pursued in nonviolent ways. The Zapatistas of Mexico have been cited as one example of activists turning to the Internet to pursue a non-violent political campaign in place of a guerrilla insurgency.[28] In other cases, the

Internet may offer a medium to facilitate conflict resolution and transformation, acting as a channel for communication across hostile lines and as a neutral forum for dialogue. The importance of people-to-people contact is being increasingly highlighted in the peacebuilding literature, though the concept is not entirely new. Allport's 'contact hypothesis' (1954) was based on the notion that, under the right conditions, constructive meetings between members of conflicting groups can alter attitudes, overcome stereotypes and promote understanding.[29] This hypothesis has proved influential. Lederach argues that sustainable peacebuilding involves working at three levels: top (high level leadership), middle-range (community leadership), and grassroots. He argues that the key to effective peacebuilding is the fostering of coordinated relationships across the levels ('horizontally') as well as between the levels ('vertically').[30] An effective medium of communication would seem to be a prerequisite for such 'bridge-building' activities. Sützl sees 'new media' as effectively occupying a similar place in conflict resolution to the traditional role of mediator; as the 'in-between space' or medium of communication between parties at all levels of society.[31] Additionally, it offers a repository of alternative information that the belligerent parties cannot control or censor. As such, the Internet offers opportunities to build the sort of 'horizontal' and 'vertical' relationships described by Lederach, allowing elite leaders, middle leaders and grassroots activists to communicate 'vertically' on their own side as well as 'horizontally' across hostile lines. Its ability to foster grassroots communication may allow ordinary people on both sides of a conflict to parley directly, bypassing belligerent leaders and perhaps offering opportunities to reduce their influence. The Internet also opens up new channels for interactions between local peacebuilding groups and international NGOs, fostering the cultural transfer of peace discourse and practices.

Allport argued that certain conditions needed to be met in order for meetings to successfully lead to change. These included both groups sending representatives of equal status; common goals; cooperation on a goal perceived as important for both parties; and authority or institutional support.[32] The Internet helps to fulfil some of these conditions. By its nature, it offers equal status and a level playing field; differences in wealth or social status, for example, are not readily apparent in cyberspace. Participants are thus able to interact freely and cooperate on the common goal of finding viable solutions to tensions and conflict. Allport's final condition, authority support, might not always be present, if by ‘authority’ we mean the local governmental or political leadership; on the other hand, the effort may be supported by ‘authority’ in the form of the broader international community, the UN and / or NGOs. The nature of the medium also helps to reduce the apprehension that people feel when they sit together with ‘the other,’ since the contact is not face-to-face.[33]

The Internet is highly resilient, even in the face of all-out conflict. Indeed, its origins are primarily based in the concept of a decentralized communications network capable of continued operation amidst wartime devastation. Due to the borderless nature of the network, information censored in one location remains available in other jurisdictions, and accessible globally. Peace activists are thus able to provide alternative information and challenge governmentally sanctioned narratives. In situations where warlike propaganda and rhetoric dominates official communications, the ability to offer an alternate perspective is of great utility. Post-conflict, the Internet can play a role in building a lasting peace culture, through the continued dissemination of ideas. It can also assist in establishing stable democracy in the aftermath of conflict, helping to facilitate transparency in elections and scrutiny of electoral processes and officials.

Although the Internet is still a relatively new development, it has already facilitated a number of practical peace initiatives. One oft-cited early example concerns the Zamir Transnational Net (ZTN), an ad-hoc Internet connection created to restore communications between Serbia and the outside world during the conflict with Croatia in 1991. Serbia’s Internet connection had been severed under UN sanctions, a move opposed by peace activists who believed this would reduce Serbians’ access to alternative sources of information. These groups took it upon themselves to create the ZTN by using borrowed telephone lines to access a server in Austria. Their intention was to boost communication between peace-oriented individuals and teams, humanitarian organisations, NGOs, independent media, and refugees and their families.[34] Eric Bachman, one of the creators of ZTN, identified a number of real benefits from the project, including the ability to pass information to foreign journalists and bypass censorship, exposure of human rights violations and increasing pressure for international intervention. Humanitarian aid groups used ZTN to coordinate their distribution of aid, and refugees were able to contact families and friends. The network also restored the possibility of direct communication between Serb and Croat peoples, helping to break down distinctions between friend and foe and allowing people to transcend some of the barriers.[35] Other analysts have highlighted the opportunities created for Western peace activists to form constructive relationships with local activists; and agree that reporting on human rights abuses may have had real effects on curbing such abuses in some locations.[36] Overall, ZTN acted as an enabler for a range of peace and humanitarian efforts, and facilitated an avenue for dialogue and civic discourse that would not otherwise have existed.

In the years following the ZTN experiment, there were further instances of Internet communication being utilised to bring groups together as part of a peace process. One example concerned Cyprus, following a 1997 decision by Turkish authorities to suspend bi-communal relations. An online peace portal called Tech4Peace was set up set up by locally based peace activists with funding from the US Agency for International Development (USAID) and the United Nations Development Program.[37] This service allowed continued interaction between organisations and individuals interested in peace and bi-communality. As a result, according to the project's creators, the momentum gained in the peacebuilding process was maintained instead of being lost.[38] A similar project trialled in Burundi during the 1993 - 2006 civil war allowed Burundians of Hutu and Tutsi backgrounds to engage in dialogue. Like the Cyprus example, these discussions provided a starting point for understanding via discussion in a physically safe online environment.[39] More recent ICT-based peace initiatives have involved participation from private sector actors such as Facebook, as well as NGOs and academic institutions. For example, a joint project set up between Facebook and the Persuasive Technology Lab at Stanford University (peace.facebook.com) aims to encourage dialogue and online relationships between opposing communities in a number of divided territories worldwide, including Israel and the Palestinian Territory, Pakistan and India, and Ukraine and

Russia.[40] Other initiatives have come from UN agencies, for example the Peacebuilding Education and Advocacy program set up by UNICEF. This involves the use of communications technology and participatory approaches to promote and deliver ‘conflict-sensitive education’ and ‘education for peacebuilding’ in fourteen countries.[41]

Advancements in technology and social media platforms are increasingly enabling victims of conflict not only to recount their experiences online, but also to evidence these by uploading high-quality photos and videos. The ability to disseminate such information may not only increase pressure for outside intervention, but could also provide a deterrent effect helping to curb abuses, particularly since such evidence might even be used to assist international prosecution. For example, the International Criminal Court used evidence from social media in issuing an arrest warrant against Mahmoud Mustafa Busayf Al-Werfalli in the context of the Libya conflict.[42] Similar evidence was made available to ICC prosecutors in a case surrounding the 2008 post-election violence in Kenya.[43]

These examples, together with various others, underline the utility of Internet technology across multiple dimensions of peacebuilding. Of course, there are currently some practical limitations. In the poverty-stricken areas of the world that are most prone to conflict, Internet access is far from universal, and even where it exists, connectivity may be lost due to war damage. Nonetheless, Internet access is rapidly increasing across the developing world,[44] and with it the network’s potential as a medium for peacebuilding work. This potential is, however, dependent upon the existence of an open Internet, where information continues to be freely shared and communication remains largely unrestricted. Such conditions should not be taken for granted, particularly in the face of numerous governments that would like to see them curtailed.

State regulation and the threat to an ‘Internet for peace’

Arguably the biggest threat to the Internet’s peacebuilding potential stems from increasing governmental ambitions to regulate and control their ‘national’ portions of the network. Again, this is borne out of ‘territorial’ thinking about the Internet. To some extent it is a reaction to the issues discussed above, but in some cases states have used security and a ‘counter-terrorism’ narrative as an excuse to justify serious attacks on online liberties. Besides creating human rights issues, this trend threatens some of the very attributes that underpin the Internet’s potential as a medium for peacebuilding and reconciliation - i.e., openness, free communication, and the ability to counter official propaganda. These attributes also make the Internet a threat to those governments whose ambition is to censor and stifle dissent.

Less than one quarter of Internet users now reside in countries where the Internet is designated ‘Free’ according to the US NGO Freedom House.[45] In many countries, content regulation extends overtly into political censorship. In a few states, such as Turkmenistan, Cuba, Myanmar and North Korea, Internet access is restricted to a small segment of the population.[46] Other governments, such as those of China and Iran, permit access but seek to restrict available content. For example, Chinese authorities have constructed a highly sophisticated, complex and multi-layered censorship and surveillance system, dedicating vast resources to the task.[47] Measures include the use of mandatory filters and website blocking, as well as other legislation regulating ISPs and content providers. ISPs are required to maintain a blacklist of banned sites, updated on an ongoing basis. In some countries, a nationalised ISP provides a single point of connection between the national network and the global Internet, making filtering and blocking easier to implement. Where there are multiple connection points controlled by several ISPs, tight management over filtering is somewhat more complicated to implement, but remains attainable given adequate regulation. In some jurisdictions, additional sophisticated technology is used, such as smart filters capable of scanning user browsing requests for banned keywords. Social media websites like Facebook, Twitter and YouTube, which permit users to share content with large audiences, are frequently restricted or blocked.[48] Besides filtering and obstruction at the ISP level, governments might also place pressure on content hosts to restrict or delete user-generated content. This might involve some degree of coercion or threat if the provider is physically located in that country. Otherwise, governments might place pressure on international hosting suppliers, often by using their complaint mechanisms to have user-generated content removed.

Overall, then, there is a general trend towards increasing national-level filtering and regulation of online content and restriction of online freedoms. Reflecting on these trends, some commentators have warned of a drift towards 'Balkanization' of the Internet, where the formerly global network becomes increasingly divided into a series of national networks, co-existing and interconnected to some degree, but with very significant restrictions on information flow between them.[49] Instead of a worldwide, borderless network, the Internet could begin to resemble the territorial map of the world, potentially losing much of its ability to facilitate cross-border communication and information exchange; i.e. the very attributes that offer a means of building bridges between conflicting parties.

Threats to Internet freedom may not remain restricted to the national level. Any shift towards greater intergovernmental control over the machinery of Internet governance may result in moves to limit online freedoms at the international level. WSIS in 2003-05 revealed a divide among governments on this issue. While the US and its allies favoured retention of the largely nongovernmental multistakeholder approach, a number of the rising powers, including Russia, China, India, and Brazil, were pushing for an intergovernmental approach that would give them greater influence.[50] A deadlock resulted, and no fundamental changes to existing Internet governance arrangements emerged from WSIS. However, states such as Russia and China continued to push for increased intergovernmentalism. Similar patterns were evident at the 2012 World Conference on International Telecommunications (WCIT) in Dubai. The purpose of this conference was to review the International Telecommunication Regulations (ITRs) that serve as the binding international treaty designed to facilitate global interconnection of data and communication services.[51] However, the event was seen in some quarters as an attempted ‘power grab’ by the intergovernmental ITU over Internet governance.[52] At the conference, a number of proposals were presented by various governments that, if successful, may have increased and legitimised censorship and surveillance. For example, several governments reportedly proposed to ban anonymous Internet usage, making it easier to find and arrest dissidents.[53] The UAE proposed amendments to the regulations granting states explicit rights to filter their Internet connections, while a submission from Algeria, Saudi Arabia, Bahrain, China, the UAE, Russia, Iraq and Sudan proposed that "member states shall have the sovereign right to establish and implement public policy, including international policy, on matters of internet governance, and to regulate the national internet segment".[54] Ultimately, the new ITR treaty was signed by 89 ITU member states, but 55 others, including the United States, Canada, Australia, the United Kingdom, and several other EU member states declined to sign. Of those states that accepted the new ITRs, the majority are classified as ‘not free’ by the Freedom in the World index (Freedom House, based in the United States) or as ‘an authoritarian regime’ by the Democracy Index (Economist Intelligence Unit, based in the United Kingdom).[55]

Despite the failure of past attempts, intergovernmentalism clearly remains the goal of a significant number of states, including some with authoritarian regimes. An intergovernmental takeover of the Internet may result in pressure from oppressive governments to shift censorship to the global level. In some respects, this could be even more damaging than 'Balkanization'. Whereas national filters can be bypassed by those with the knowledge and skills to do so, a centralised censorship regime would be far more difficult to evade. For this reason, moves towards an intergovernmental model of Internet governance must be resisted. While multistakeholder institutions such as ICANN are far from perfect - and there are legitimate considerations over corporate capture of their multistakeholder processes - an intergovernmental takeover should not be seen as the solution to these issues.

The Nongovernmental Alternative

Rather than viewing the nation-state as the appropriate locus for an Internet security strategy, it would be more appropriate to focus on securing the network at global level. This would require overhaul and strengthening of the Internet's governance mechanisms, leading to the establishment of a consolidated Internet authority. An authoritative centralised governing body would reduce the condition of anarchy that currently characterises the network. This would help to negate those consequences that realists believe must necessarily flow from anarchy, including uncertainty, self-help and the security dilemma.

Instead of the intergovernmental organization desired by some states, this new Internet authority could be organized in accordance with the existing multistakeholder principle. Its key responsibilities with regards to securing the network would be twofold. The first would be to secure essential core systems against the likelihood of cyberattack, while the second would be to actively police the network to counter threats. A high degree of co-ordination between technical and corporate stakeholders would be required, involving data sharing and joint action to find, assess and deal with emerging cyber threats on the global network. To a considerable degree, responsibility for securing various aspects of Internet infrastructure already rests with private stakeholders and multistakeholder governance bodies. Securing the root nameservers, for example, is one of the core responsibilities of ICANN. ISOC, too, has recognized its responsibilities in this area, working with different bodies to develop concrete policy solutions for securing the Internet, and facilitating discussions around definitions and understandings of cybersecurity involving both public and private actors.[56] Various private stakeholders have also joined together to launch cybersecurity initiatives. In 2017, for example, a group of major Internet companies, including Facebook, Microsoft, Twitter and YouTube, formed the Global Internet Forum to Counter Terrorism. This initiative formalises and structures how these companies work together to curtail the sharing of terror related and extremist material on their hosted consumer services, as well as fostering collaboration with smaller tech companies, civil society groups, academia, and governments.[57] Cybersecurity is also a significant topic of discussion at the Internet Governance Forum, the multistakeholder platform set up to continue discussions following WSIS.

Such initiatives represent tentative steps in the right direction. However, there is a need to go further, by building consolidated and robust governance machinery with an emphasis on security. A consolidated and centralized Internet governance body would have the authority and scope to develop an integrated security strategy at global level. Implementation of this policy would require co-ordination between relevant stakeholders, such as ISPs, social media providers, webhosts, email providers and name registrars. In turn, those stakeholders would participate in the central authority and have a voice in developing its policies. The governance agency could be endowed with a range of powers to respond to security threats. For example, it could order the permanent or temporary suspension and blocking of particular domains, IP address ranges, websites and social media platforms, and even physical connections. It might invoke specialist agencies with the technical expertise to infiltrate extremist organisations online and gather intelligence on emerging threats. Such agencies could develop technical counters to known cyberweapons and methods of cyberattack, or could even be authorized to proactively take down known online assets of a threatening organization. Several such approaches are already being actively pursued as elements of national cybersecurity programs, but could be considerably more effective if co-ordinated at global level.This is not to suggest, of course, that any possibility of using the Internet for destructive purposes would be entirely negated. Nonetheless, a new global authority with the powers described above would represent the establishment of an unprecedented level of 'law and order' on the network.

The major obstacle to implementing a consolidated and centralised nongovernmental Internet governance authority may be resistance from states. The concept of non-governmental governance and authority at the global level is by no means without precedent, either in academic theory or in practice. Numerous private regulatory and rule-setting mechanisms and structures have emerged across a wide range of issue-areas, a phenomenon well documented by scholars.[58] In International Relations scholarship, efforts to redefine and reinterpret security in nonstate terms have an established history. There is a great volume of literature, particularly from critical security studies theorists, arguing that the ultimate referent objects of security should be individuals, rather than states.[59] Despite these scholarly innovations, traditional conceptions of ‘national security’ are still deeply entrenched in the mindset of governments. Persuading those governments to relinquish control of an issue they have framed in ‘national security’ terms, and hand that responsibility over to a nongovernmental authority, is likely to be very difficult. Rather than attempting to convince governments, therefore, the best way forward might be for the Internet governance community to proceed without them.

As demonstrated at WSIS and WCIT, any attempt to create a new Internet governance authority via the ITU would prompt attempts by a number of states to secure an intergovernmental takeover. While such efforts would be resisted by the United States and its allies, this would once again result in the sort of stalemate that rendered those previous summits largely fruitless. Instead, the initiative could come from the existing Internet governance bodies themselves, particularly from ISOC and ICANN, and from the major stakeholders in the industry. In considering the design of the new body, some thought could be given to inclusion of a permanent element of elected representation for the Internet-using public. This idea would not be without precedent. In ICANN’s original incarnation, there was a mechanism whereby a proportion of the organisation’s governing Board of Directors was directly elected by the global Internet-using community. This mechanism was abandoned by ICANN, but the principle could be integrated into the design of a new consolidated Internet authority. Such an element of elected representation would arguably confer greater legitimacy upon the new organization. It would act as a bulwark against capture either by corporations or powerful governments, and would help to ensure that the voices of previously marginalized groups – those in greatest need of an ‘Internet for Peace’ – would be heard. It would also help to reinforce the lesson that there are genuine possibilities for political organisation beyond the territorial nation state.

Conclusion

Matters of Internet governance are of real significance for global peace and stability. Whether the Internet will prove to be a destructive and destabilising force or a true ‘weapon of mass construction' in the years ahead is very largely dependent on the governance structures that are set up to control it, their nature and purpose, and ultimately the underlying conceptual understandings and frameworks that underpin them.

Since governments first came to identify 'national' interests in Internet governance, they have tended to approach the issue-area in what might be deemed 'realist' terms, especially with regards to 'national security'. To some extent, some basic realist assumptions are applicable to the medium. In its current state, the Internet does indeed represent a system of anarchy, with no strong central governing body, and an ongoing competition among actors to maximise their individual power and capability in cyberspace. Under such conditions, it is only prudent for actors to distrust each other's intentions. Beyond this, though, the inapplicability of 'statist' conceptualisations of security to a borderless global medium is clear, yet governmental responses to issues of cybersecurity remain rooted in deeply entrenched 'realist' models. In applying such assumptions, though, governments actually make themselves - and everyone else - less secure. In an arena that fundamentally is not about national territories, where capabilities and balances of power are uncertain and subject to rapid change, and even the identities and nature of the actors might be uncertain, there are real dangers in trying to apply wholly inappropriate 'realist' thinking. Realism may indeed become a self-fulfiling prophecy, its assumptions prompting governments to enter into cyber-arms races and in doing so only amplifying the conditions of uncertainty and the likelihood of conflict. Furthermore, efforts to divide up control of the Internet on 'national' lines also threaten the network's potential to be used as a positive channel for peacebuilding. The Internet has already proved its immense value as a peacebuilding tool and, given the right conditions, its potential to help overcome division and conflict should continue to increase as an ever larger proportion of the world's population gets online. However, this is conditional on the network remaining open, with communication remaining unrestricted across borders and lines of conflict.

While 'cyber-realist,' territorially based responses are unhelpful, there is an alternative route towards creating stability while preserving the Internet's open and borderless nature. This lies in overcoming the conditions of anarchy that exist in the online realm, by finding a means to create order and centralised authority. At first glance, intergovernmental diplomacy might seem to be the obvious way to accomplish this. A multilateral agreement among governments might help to reduce uncertainty to a degree, by setting some principles, norms and expectations around cyberwarfare and acceptable state conduct in cyberspace. However, this would not necessarily be straightforward, and a purely intergovernmental approach faces obvious limitations, especially since nonstate actors would not be bound by interstate treaties. Furthermore, any intergovernmental takeover of Internet governance could give a powerful voice to authoritarian governments, and this may also threaten online freedoms. Any such moves should, in the author's opinion, be vigorously opposed.

To truly overcome anarchy and build a central authority appropriate to the Internet, there is a need to move away from statist thinking altogether and focus on alternative models. The Internet was, from the outset, a pioneering experimental testbed for multistakeholder approaches to governance. Building on this foundation, a centralised and consolidated Internet authority could be achieved through integration of the existing multistakeholder partnerships. However, while the notion of nonstate governance is by no means a new idea, the prospect of entrusting a 'security' matter to a nonstate authority would require a monumental shift in thinking on the part of governments. Realistically, therefore, the only way forward would probably be for the Internet governance community itself to take the initiative. Rather than waiting for squabbling governments to provide leadership, the existing stakeholders are the actors in the best position to create the required order. Via the already existing institutions, the community itself has the organisational capacity to make progress on this matter, and indeed also has a clear duty to recognise its responsibilities in this area.

Of course, any such new authority must be seen to have legitimacy. In the absence of intergovernmental oversight, an alternative basis for legitimisation would lie in strengthening the voice of civil society in the organization, perhaps even incorporating the sort of electoral mechanism previously trialled by ICANN. Such a mechanism would create a powerful 'public interest' stakeholder bloc as a check against the ambitions both of authoritarian governments and overmighty corporations. Civil society groups, including the academic and peacebuilding communities, have an opportunity to take a leading role in helping to construct this new governance structure. Peacebuilders can help to articulate a vision for a future Internet that remains open and free from state censorship and control, but at the same time is safeguarded— to the greatest extent possible—against misuse.

There is a vitally important need to bring awareness of these issues to peace scholars and peace practitioners. However, mere awareness of the issues is not enough. There are many avenues by which individuals and organisations can become actively involved in the multistakeholder Internet governance system and help to steer its future direction, for example through the IGF, through ICANN's public participation mechanisms, and through ISOC. In addition, citizens of democratic states can petition their governments to support multistakeholder reform and oppose any moves towards governmental takeover that could legitimise and enable censorship and undermine online freedoms. These issues are of real and urgent importance, not only for the Internet governance community but for international peace and stability. The International Relations and peace studies communities should be ready to play an active role in achieving 'cyberpeace.'

References

[1] UNWGIG. *Report of the Working Group on Internet Governance* (New York: United Nations, 2005) http://www.wgig.org/docs/WGIGREPORT.pdf

[2] Yochai Benkler, "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access," *Federal Communications Law Journal* 52, no. 3 (2000): 561-579.

[3] "Convention on Cybercrime" Opened for signature November 23, 2001. *European Treaty Series* no. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[4] John Mathiason, *Internet Governance: The new frontier of global institutions* (New York: Routledge, 2009), 97.

[5] ITU, "World Summit on the Information Society - Declaration of Principles," WSIS-03/GENEVA/DOC/4-E, December 12 2003, Article 49, http://www.itu.int/net/wsis/docs/geneva/official/dop.html

[6] Mathiason, 124.

[7] Ines von Behr, Anais Reding, Charlie Edwards and Luke Gribbon, *Radicalisation In The Digital Era: The Use Of The Internet In 15 Cases Of Terrorism And Extremism*. (Santa Monica: RAND Corporation, 2013). http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

[8] Gabriel Weimann, *Terror on the Internet: The new arena, the new challenge* (Washington D.C.: United States Institute of Peace Press, 2006), 9.

[9] Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *Journal of Slavic Military Studies* 27, no. 1 (2014): 105-106.

[10] Anke Schmidt-Felzmann, "After the war in Ukraine: peace building and reconciliation in spite of the external aggressor," in *International Crisis Management: NATO, EU, OSCE and Civil Society,* ed. Goda, S. et al (Amsterdam: IOS Press, 2016), 151.

[11] NATO, "Wales Summit Declaration," September 5 2014, Article 74, https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[12] James Andrew Lewis and Götz Neuneck, *The Cyber Index: International Security Trends and Realities* (New York and Geneva: UNIDIR, 2013).

[13] Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (2013): 366.

[14] Tim Maurer and Scott Janz, “The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context,” *International Relations and Security Network,* published October 17 2014, http://www.css.ethz.ch/en/services/digital-library/publications/publication.html/187945

[15] Volodymyr Lysenko and Catherine Brooks, “Russian information troops, disinformation, and democracy,” *First Monday* 23 no. 5 (May 2018) http://dx.doi.org/10.5210/fm.v23i5.8176

[16] Stephen M. Walt, "International Relations: One World, Many Theories," *Foreign Policy,* no.110 (Spring 1998): 29

[17] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton, 2001).

[18] Kenneth N. Waltz, *Theory of International Politics* (New York: McGraw-Hill, 1979).

[19] John H. Herz, “Idealist Internationalism and the Security Dilemma,” *World Politics* 2, no. 2 (1950), 157–180.

[20] Charles L. Glaser, “When Are Arms Races Dangerous? Rational versus Suboptimal Arming,” *International Security* 28, no.4 (2004): 44–84.

[21] James Andrew Lewis and Götz Neuneck, *The Cyber Index: International Security Trends and Realities* (New York and Geneva: UNIDIR, 2013), 3.

[22] Anthony Craig and Brandon Valeriano, “Reacting to Cyber Threats: Protection and Security in the Digital Age,” *Global Security and Intelligence Studies* 1, no. 2 (Spring 2016):21-41.

[23] Hans Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1978), 5.

[24] Waltz 1979: 131

[25] Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), 123

[26] Hyeong-wook Boo, “An Assessment of North Korean Cyber Threats,” *The Journal of East Asian Affairs* 31, no. 1 (2017): 197-117.

[27] John C. Abell, "Internet 'in-running' for Nobel Peace Prize," *Wired*, last updated March 2010, https://www.wired.com/2010/03/internet-in-running-for-nobel-peace-prize-bbc/ , accessed 8/3/2017

[28] Gabriel Weimann, *Terror on the Internet: The new arena, the new challenges.* (Washington D.C.: United States Institute of Peace Press, 2006), 12.

[29] Gordon W. Allport, *The nature of prejudice* (Reading, MA: Addison– Wesley, 1954).

[30] John Paul Lederach, *Building Peace: Sustainable Reconciliation in Divided Societies* (Washington, D.C.: United States Institute of Peace Press, 1997).

[31] Wolfgang Sützl, "Elicitive Conflict Transformation and New Media: In Search for a Common Ground", *Media and Communication* 4, no. 1 (2016): 4-5.

[32] Allport, 281.

[33] YairAmichai-Hamburger and Katelyn Y. A. McKenna McKenna, K. Y. A., "The contact hypothesis reconsidered: interacting via the internet," *Journal of Computer-Mediated Communication* 11, no. 3 (2006): 829-830.

[34] Amy Herron and Eric Bachman, "Zamir Transnational Net: Computer-Mediated Communication and Resistance Music in Bosnia-Herzegovina, Croatia and the Federal Republic of Yugoslavia," in *Culture and Technology in the New Europe: Civic Discourse in Transformation in Post-Communist Nations*, ed. Laura B Lengel (Stamford, Conneticut: Ablex Publishing Corporation, 2000), 273-292.

[35] Ibid, 8.

[36] Paul Stubbs, "Conflict and Co-Operation in the Virtual Community: eMail and the Wars of the Yugoslav Succession," *Sociological Research Online* 3, no. 3 (September 1998): 3.2-3.9. http://www.socresonline.org.uk/3/3/7.html

[37] Yiannis Laouris, "Information Technology in the Service of Peacebuilding: The Case of Cyprus," *World Futures* 60, no. 1-2 (2004): 74.

[38] Romina Laouri, "Using technology to promote communication and peace-building activities in Cyprus," Paper presented at the 2007 War and Poverty, Peace and Prosperity Conference at the Levy Economics Institute of Bard College, Annandale, New York, June 2007.

[39] Rose M. Kadene Kaiser, “The transformation of discourse online: Toward a holistic diagnosis of the nature of social inequality in Burundi,” in *Native on the Net: Indigenous and Diasporic Peoples in the Virtual Age,* ed. Kyra Landzelius (New York: Routledge, 2004),226.

[40] Orna Young and Edna Young, *Technology for Peacebuilding in Divided Societies* (Belfast, Northern Ireland: Transformative Connections Organisation, 2015), 31.

[41] Monica Llamazares and Katie Mulloy, “Unicef in Uganda: Using Technology-Based Innovations to Advance Peacebuilding,” *Journal of Peacebuilding & Development* 9, no. 3 (2014): 109.

[42] Emma Irving, “And So It Begins… Social Media Evidence In An ICC Arrest Warrant,” *Opinio Juris*, August 17 2017, http://opiniojuris.org/2017/08/17/and-so-it-begins-social-media-evidence-in-an-icc-arrest-warrant/

[43] Patrick Meier, “Ushahidi as a liberation technology,” in *Liberation Technology: Social Media and the Struggle for Democracy,* ed. Larry Diamond, Marc F. Plattner (Baltimore: John Hopkins University Press, 2012), 97.

[44]"Individuals using the Internet (% of population)", *World Bank Group,* https://data.worldbank.org/indicator/it.NET.user.ZS, accessed 1/10/2019.

[45] Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp, and Jessica White, *Freedom on the Net 2017* (Washington, D.C.: Freedom House, 2017).

[46] Daniel Calingaert, "Authoritarianism vs. the Internet," *Hoover Institution Policy Review*, April 1 2010. http://www.hoover.org/research/authoritarianism-vs-internet

[47] Sanja Kelly and Sarah Cook, *Freedom on the Net 2011: A global assessment of Internet and digital media* (Washington, D.C: Freedom House, 2011), 88.

[48] Ibid, 3

[49] Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (London: Hachette UK, 2013), 85.

[50] Mathiason, 124.

[51]“World Conference on International Telecommunications (WCIT-12),” *International Telecommunication Union,* published December 2012, http://www.itu.int/en/wcit-12/Pages/default.aspx, accessed 7/30/2017.

[52] Lynn Stanton and Brian Hammond, “U.S. officials emphasize opposition to ETNO proposal, while ITU officials protest 'myth' of Internet takeover plan,” *Telecommunications Reports* 78, no. 20 (2012): 14-18.

[53] Vinton Cerf, "'Father of the internet': Why we must fight for its freedom," *CNN Editorial*, published November 29 2012, http://edition.cnn.com/2012/11/29/business/opinion-cerf-google-internet-freedom/index.html

[54] Richard Hill, *The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History* (Berlin: Springer Science & Business Media, 2014), 61.

[55] Tim Maurer and Robert Morgus, “Tipping the Scale: An Analysis of the Global Swing States in the Internet Governance Debate,” *Centre for International Governance Innovation Internet Governance Papers* no. 7 (May 2014) https://www.cigionline.org/sites/default/files/no7_2.pdf, 6

[56] “Cybersecurity: Searching for a Common Understanding,” *Internet Society*, published March 2013, https://www.internetsociety.org/resources/doc/2013/cybersecurity-searching-for-a-common-understanding/, accessed 8/15/2018.

[57] “Global Internet Forum to Counter Terrorism to hold first meeting in San Francisco.” *YouTube Official Blog,* published July 2017. https://youtube.googleblog.com/2017/07/global-internet-forum-to-counter.html

[58] Rodney Bruce Hall and Thomas J. Biersteker, “The emergence of private authority in the international system.” in *The Emergence of Private Authority in Global Governance*, ed. Rodney Bruce Hall and Thomas J. Biersteker (Cambridge, Cambridge University Press, 2007), 3-22.

[59] Ken Booth, *Critical Security Studies and World Politics* (Boulder, Colorado: Lynne Rienner Publishers, 2005)