# The Edinburgh Companion to Political Realism

Edited by Robert Schuett and Miles Hollingworth


EDINBURGH
University Press

Edinburgh University Press is one of the leading university presses in the UK. We publish academic books and journals in our selected subject areas across the humanities and social sciences, combining cutting-edge scholarship with high editorial and production values to produce academic works of lasting importance. For more information visit our website: edinburghuniversitypress.com



Edinburgh University Press Ltd
The Tun – Holyrood Road
12(2f) Jackson's Entry
Edinburgh EH8 8PJ

Typeset in 10/12 Adobe Sabon by
IDSUK (DataConnection) Ltd, and
printed and bound in Great Britain.

A CIP record for this book is available from the British Library

ISBN 978 1 4744 2328 1 (hardback)
ISBN 978 1 4744 2329 8 (webready PDF)
ISBN 978 1 4744 2330 4 (epub)

# Contents

**Part III: Political Realism and Foreign Policy**

# 42

# Political Realism and the Internet

## New networks of power

*Richard Forno*

## Chapter Overview

Technological developments such as the internet, smartphones and social media offer individuals and organisations alike the power to develop, strengthen and/or exploit common interests and group capabilities through shared community participation. But through this process and these technologies, communities can also become selectively informed, intensely fragmented and, ultimately, at odds with each other. The 2016 US presidential election offered a global glimpse of such effects upon both Western democratic political processes and the foundations of society more broadly. This chapter explores the nature of power within the modern networked society. By situating the discussion within this decentralised information environment, it examines how the sources of social authority and political power – in other words, the capacity to create widespread tangible outcomes – have become flattened, with new sources of meaningful social influence arising at the network's edges – a situation which the author presents as the 'authorisation-availability' dynamic regarding the flow of networked information. Using two examples from internet history, he discusses how these network-level entities challenge existing sources of social and political power and create a conflicting cycle of outcomes as the old power paradigms are challenged. Ultimately, the author warns that, despite the potential for dramatic shifts or upheavals in the application of social power through decentralised networks and technological developments – which remains a cherished Gibson-esque cyberpunk notion, radical shifts in the balance of power in society are possible but not assured; however, a constant tension remains between the actors involved.

* * *

Technological advancements, from the telegraph and the telephone to the internet and social media, continue to serve as useful tools for government entities, as well as politicians, their supporters and lobbyists, and individual citizens. They allow for the expression of views and the planning or conduct of political action. While the so-called 'Dot Com Revolution' of the late 1990s introduced global, easy-to-use communication capabilities to the public that once were possessed only by governments and large corporations, the controversial American presidential election of 2016 served as a

clear demonstration of the potential of such internet-centric technologies to influence – though some might say determine – the outcome of political processes and to craft assorted political realities.

This means that such powers as were once maintained and exclusively wielded by governments, militaries and large media companies have become decentralised, so that individuals and unstructured groups now have the ability to create, collect, analyse and distribute information and knowledge in ways that rival, if not surpass, the traditional sources of knowledge-power, information distribution and social, legal and political authority.

Much continues to be written about the 'networked society' and how information technologies bridge the proverbial 'tyranny of distance' to bring the world closer together, to craft communities and to foster collective action. Indeed, politics and power are functions of society and human nature, just as the possible applications of technology are determined not by the existence of the technology itself but by the intent of its human users. Therefore, this chapter will explore some of the consequences of internet ('cyber') capabilities vis-à-vis the question of power and society. Specifically, it will discuss the relationship of social authority and political power to internet technologies and the resulting effect upon the flows of internet-based information. Presuming that 'knowledge is power', it will discuss how such technologies can foster greater global public information flows that can lead to shifts in power and influence vis-à-vis their traditional sources: not just once, but in an ongoing and accelerating manner. However, before discussing these issues, a brief introduction must be made of some of the technical aspects of the internet that facilitate these outcomes.

## The Architecture of Decentralised Information

What is today called the internet can be traced back to the Cold War era of the mid-twentieth century and a desire by the USA to develop a network for military command and control that could survive a nuclear exchange with the Soviet Union (Abbate 1999; Leiner et al. 2003). At that time, engineers believed that such a network had to be decentralised so as to offer adversaries no single point of vulnerability, no single target, to disrupt, degrade or destroy its communications links during wartime.

Unlike traditional communications networks that required a dedicated point-to-point connection for each message exchanged, this survivable network environment was developed under the principle of distributed communications that allowed messages transiting its network to flow across different pathways simultaneously to reach their ultimate destinations. A key benefit of this technique for message handling was that a communications path between individual network nodes did not require a continuous network line to remain open; once a message transited a pair of nodes, the path was released to accept other messages. It was this feature of network and message resiliency that appealed to engineers as they refined their designs for an information infrastructure that could survive a nuclear war even if individual nodes were destroyed or otherwise unreachable. It would also go on to define one of the key social consequences of the internet's use in contemporary society. Indeed, a common refrain during the early days of the commercial internet was that 'the network routes around obstacles'.

In fact, it was in these early days of the Advanced Research Projects Agency Network (ARPANET) that e-mail distribution lists (listservs) were invented that allowed a single user to broadcast messages to multiple other network nodes with ease, thereby enabling the individual network user to become their own publisher of information to others. As Abbate (1999) notes in her seminal work on the history of the internet, 'email laid the groundwork for creating virtual communities throughout the network' and people would come to see the ARPANET 'not as a computing system but a communications system'. Of particular significance is the realisation that the evolution of the internet from its original purpose of a time-sharing resource (ARPANET) to one whose primary function was – and remains – communications, demonstrates how technology can evolve in manners far different from its designers' original intentions, the only limitations on the extent of this evolution being how innovative its users are and how the technology itself is embraced. Ultimately, ARPANET evolved into the present-day internet, complete with networked personal computers, mobile devices, social media, virtual private networking, peer-to-peer communications and more, serving as a dominant resource for public interaction around the world.

## The Authorisation–Availability Dynamic

In his early writings on information flows, Manuel Castells suggests that networks and networking may provide the impetus for radical change in the traditional notions of society, social organisation and sources of social power (Castells 2000). To Castells, the networked environment is a 'space of flows', where capital, information and social organisations exist and evolve. Because such networks are not constrained by geographical locations and rigid processes, he suggests that these networked flows contribute to the 'destruction of human experience', in that, among other things, the ability to achieve influence and authority over others is separated from the traditional sources of political power. In discussing the effect of such flows on the nation-state and the international political system, and the potential for redefining the sources of authority and influence within them, Castells (1996) warns that 'nation states will survive, but not so their sovereignty'. More specifically, he writes that the network enterprise is 'that specific form of enterprise whose system of means is constituted by the intersection of autonomous systems of goals'.

If one presumes that information and knowledge are used as tools to gain and maintain political power in society, two factors regarding the networking of information come to mind. The first influence on network flows relates to the original release of owned information. This can exist in the form of *granting or withholding authorisation* for others to access information by its owner(s) on either a partial or a complete basis or until certain conditions have been met. For example, an e-book publisher may embargo the sale of a new novel until a certain date and time as part of its worldwide marketing campaign – but selectively release advance excerpts to generate sales interest. Or, a mobile service company may choose to withhold the public release of information pertaining to its quality of service, believing that such information is proprietary and could provide marketplace competitors with an advantage in challenging it to gain customers. Similarly, a software manufacturer may allow third parties to

have detailed technical access to its product information or programming interfaces to enable them to build complementary products yet withhold such access from the general public. At a national or political level, governments often withhold (also called 'classify') the disclosure of information (such as military plans or diplomatic initiatives) to protect their national secrets, limiting access only to those individuals who are cleared (that is, approved) to access that information. Of course, in other cases, information owners may give authorisation for the free release of their owned information without any restrictions or conditions whatsoever – such as a published government study or the advance book excerpts mentioned earlier. In other words, the decision to grant or withhold the release of information is based on the motivations and perceptions of the information owner.

However, once information is released, *how it exists and flows* within that community must also be considered. For example, although a company may restrict the public disclosure of certain information, that information may become publicly available through a disgruntled employee or corporate whistleblower – at which point, the information has moved beyond the company's boundary and away from an area under the company's easy ability to control or influence. Some internet websites, such as Wikileaks.Org, specialise in and are infamous for providing an internet resource for such information to exist and to be made available to the general public which is not easily restricted or disabled by information owners.

Conversely, information may exist and be available in an unrestricted form, but this fact alone will not guarantee its flow across the network if public attention is not first drawn to its presence.

Consider the amateur playwright who places a script on the public portion of his internet website. Although his act of making the script public grants the internet population the ability to access his product, if he does not take steps to advertise his website and attract attention from the internet population, he is not enabling his resource – his script – for wider networked flows and reaching its desired target audience. In a similar way, data or knowledge – such as scientific data or financial reporting materials – may be uploaded into a public repository or library for anyone to access. Therefore, information 'availability' refers not to the granting or withholding of authorisations to access information, but rather to the sheer reality that such information exists on the public network and users are able to obtain it.

Although the owner of an information resource may exercise control over it and grant authorisation for its use within its organisational boundary – such as a company or agency network or facility – once that information moves beyond that organisation's legal or technical ability to control it (even only briefly), the source organisation's ability to influence its flow across a network or grant authorisations for its use can then be severely, if not hopelessly, limited. The latter is especially true when discoveries are made about privately owned information by third parties such as Wikileaks, commercial media, or independent entities not easily influenced or coerced by information owners to restrict or remove that knowledge from public view.

As such, any discussion of information and knowledge flows on the internet would be incomplete without mentioning the phenomenon unofficially named the 'Streisand Effect' – namely, when a request to restrict the flow of information already existing on the network becomes publicly known, such as through a publicised legal takedown

order or request by a government entity to remove something from the public internet (Arthur 2009). This request, once it becomes known, tends to generate increased interest in that information from others, including those with no previous interest in the information in question and who are simply curious. Over the years, in both political and commercial spheres, there have been many high-profile cases in which news of the attempted restriction of information flows on the internet has spawned a network response in protest that then went on to propel the information even further into public view – most notably, in cases where several internet users believed they were witness to or victims of abusive applications of commercial intellectual property laws. More recently, in late 2016, fearing the deletion of troves of government scientific research data following a series of national victories by perceived anti-science, anti-knowledge political parties, American researchers began a prolonged and wide-reaching effort to mirror publicly available government data in third-party systems, since that information was believed to run contrary to the incoming administration's partisan ideology and could be targeted.

## Power Challenged

In examining these two influences upon the flow of information and knowledge in society, several recurring conditions of controversy between network participants become evident. Arquilla and Ronfeldt (1997) argue that 'the information revolution . . . disrupts and erodes the hierarchies around which institutions of power and authority are normally designed. It diffuses and redistributes power, often to the benefit of what may be considered weaker, smaller actors.' Although physical resource owners have maintained dominant control over their properties through traditional methods of tangible property ownership, the internet has challenged, if not changed, the paradigm of how new, information-based properties (such as movies, music, embarrassing videos, leaked political information and more) are controlled. It presents new opportunities for conflict between information owners and those who are able to influence those properties, and it generates new methods and codes of conduct that are largely determined and driven by social expectations. Indeed, this suggests questions over how, or if, information ever can be constrained completely by its owners in a manner similar to the ownership of physical resources. By extension, this can challenge the viability and effectiveness of traditional social organisations (such as governments, corporations or industry cartels) that are based on rigid social hierarchies of resource control and community authority.

From an anthropological perspective, Rose (1999) has observed how the internet has helped to divide large population blocks in society into smaller, niche elements that in turn become the building blocks for new flows and relationships. All of this is to say that the internet has helped to trigger bottom-up changes to the traditional methods of social interaction and authority. In other words, networks, as a social and technological construct, can present an opportunity to challenge the traditional centres of social authority, while new information flows can go on to lead to the development of new networks and forms of interaction altogether. A similar sentiment is expressed by Dyer-Witheford (1999), who equates these networks with the proliferation of fringe groups, minorities and other such movements, eager to appropriate these new methods

and mechanisms that so clearly lie outside the norms of traditional social organisation and authority. In such cases, information-based resources, news, products or knowledge are distributed in a complex and decentralised fashion, rather than exclusively in the vertical, top-down method that has been favoured by the traditional corporate, social and political powers. Indeed, the rise and purported public acceptance of alternative 'news' sources, so-called 'alternative facts', and information repeated within partisan echo chambers during the 2016 American presidential election, demonstrate the power and speed of this 'network effect' as it unfolds between participants possessed of varying degrees of prominence, legitimacy and contextual understanding.

Just as the internet's design allows it to accommodate an increasing user population along with new technologies to create or exchange information, those within a networked social environment can utilise innovative technology to form new networks, change older ones or evolve their current network into something newer to meet their snowballing information-based needs. Arquilla and Ronfeldt (2001) consider this to be an example of 'networks fighting networks' and something that John Urry (2004) identifies as the difference between the 'egalitarian web' and an 'aristocratic pattern'. Urry notes that the latter is an attempt by the power centres in a given network to attempt to manage the unfolding complexity and expand their own ability to influence the network through the traditional methods of top-down influence. However, we are seeing a number of examples now in which the design of the network itself precludes this from occurring. Indeed, as mentioned earlier, during the 2016 American elections, diverse political communities embraced the capabilities of decentralised networks – both technological and social – to further their agendas in the face of established regimes of social authority and information, such as the mainstream media and academia.

Notwithstanding all of this, we must remain cognisant of the fact that, while networks are inseparable from hierarchies and sources of power, and may lead to increasing gaps between social authorities and individuals, there remains a possibility that the changes to society that they bring about might actually *reinforce* the existing social organisations and their mechanisms of control. Notice that in everything we have discussed thus far, *power* has been at the forefront. The internet remains very much a 'human' technology. Its rapid effect upon society shows us that it is, in fact, mirroring and magnifying certain aspects of human nature which have been there all along. So far, this has been somewhat disguised by the fact that the standout examples of the internet's new networks of power tend to feature the 'old order' being outwitted and outrun by the 'new order'. But 'power is power', and if the internet and its networks are one of power's major new sources and arenas, then we may simply be witnessing the old conflicts in their new, most public, dimension. Examples of two such conflicts – and their political consequences – are discussed next.

## An Antagonism of Outcomes

First, let us examine the failed attempt by the US government in 1993 to restrict from the rest of the world the distribution of a new and significantly stronger form of cryptography called Pretty Good Privacy (PGP). Phil Zimmerman, the creator of PGP, was pursued by federal law enforcement after copies of PGP began appearing on internet

newsgroups without Zimmerman first obtaining federal approval to 'export' (in other words, move beyond its national borders) technology that the US government considered a controlled military munition. By refusing to authorise the export of PGP, the government showed that it believed the widespread availability of PGP's advanced encryption capabilities represented a significant danger to its ability to intercept electronic communications – particularly those of foreign countries. Underscoring this situation was the government's belief that it could control the distribution of defence-related information on the internet in the same manner as it could control the distribution of defence-related items used in the physical world, such as missiles, explosives or other weaponry: in the sense that we have an 'item' and we lock it away in a room that few – and only the proverbial 'good guys' – can access. However, soon after its initial release on the internet, the computer code for PGP appeared and was exchanged on an increasing number of internet sites around the world.

As a result, a conflict between the issues of authorisation and availability became clear. Although the US government desired to restrict the distribution of strong encryption capabilities as part of its national security responsibilities, PGP was obtainable by anyone in the world connected to the internet. Furthermore, once the government began legal proceedings against Zimmerman for distributing PGP and openly tried to remove the software from public access, internet users around the world worked to keep PGP publicly available in the belief that such capabilities were necessary to foster greater personal privacy for global electronic communications – thus demonstrating the 'Streisand effect'. Consequently, PGP remained outside of the US government's ability to retrieve, suppress or otherwise restrict its distribution to others as part of its national security interests or desired policy. Anyone and everyone, everywhere, now had access to this software code, deemed a critical national security capability.

This situation demonstrated to world governments and internet users alike that the internet and related communications technologies can make the traditional methods of restricting the widespread distribution of information, such as simply including it on a national list of prohibited items, obsolete. In the years following the PGP event, similar situations occurred when emerging technologies challenged government attempts to control the worldwide public distribution of other types of sensitive or restricted information, such as highly detailed satellite images from commercial companies, the location of nuclear power plants, government reports and documents, questionable personal videos and even commonly known scientific facts. In most cases, these actions were begun in the belief that information placed on the internet could be retroactively recalled or restricted (Card 2002). As recently as 2016, Western politicians continue offering speeches and legislative initiatives suggesting that keeping public knowledge out of view is a viable tool of security and a doable outcome. More so, some national governments still attempt to restrict, reclaim or remove from the internet items deemed controllable – such as the Thai government's ongoing attempts to apply their *lèse-majesté* laws to 'prohibit viewing' (or even the deletion) of information it deems embarrassing for their citizens to see, regardless of where in the world they are or how they are accessing it (Moody 2017).

The PGP example also provides insight into the distinctions between 'know-how' and 'know-that', made by Gilbert Ryle (1946) and Karl Polanyi (1966) when describing information restrictions and social authority. While a government might

wish to restrict the public distribution of strong encryption, encryption itself is a mathematical process. Unless it is able to restrict public know-how about complex algorithms and applied mathematics, or prohibit the human actions of research and enquiry, in reality, such restrictions never can be fully enforced. Even if the government creates its own secret encryption technology (that is, proprietary 'know-that'), there can be no guarantee that researchers around the world could not, of their own volition and based on their own competencies, derive the 'know-how' behind that restricted information and either publicise it anyway or develop their own technologies. Again, it is quite difficult to criminalise the discovery or application of knowledge, both on the internet and in human society. Thus, in terms of power and political realism regarding cyber issues and technology, the PGP example shows that situations can develop in which information is exchanged, even when others might prefer it be restricted.

Our second example demonstrating the authorisation-availability dynamic and the resulting shift in power outcomes relates to attempts to constrain the public knowledge of technology 'know-how' from the entertainment domain. In the late 1990s, to prevent emerging internet technologies from facilitating the global piracy of digital movies and music, the entertainment industry developed technical methods (known as digital rights management, or DRM) to ensure that each digital file (music or movies) purchased could be played only on a finite number of devices or could not be copied (that is, pirated) to others unless it received additional payments for those copies. DRM was intended to make these non-rivalrous digital items rivalrous – and therefore, to try to make their distribution controllable by their owners in an attempt to protect their rights of ownership in this new digital marketplace. Nevertheless, customers still viewed digital music and movies they had purchased as 'theirs' and sought methods to use and enjoy these digital items in the same manner as they did with music obtained from physical media such as records and compact discs: all despite the music industry's reluctance to embrace internet technologies such as MP3 formats or streaming. Further, DRM was envisioned by entertainment companies as a way to maintain their marketplace role as the primary purveyors and distributors of entertainment media – and thus preserve their top-down legitimacy in an increasingly decentralised customer and content-generation marketplace.

In response, sites, services and products quickly emerged to facilitate the widespread distribution of digital entertainment products that were unencumbered by DRM and allowed customers to treat such products as 'theirs', even if legally they were not. If DRM was intended for use by rights owners to transform their non-rivalrous digital resources into rivalrous ones to protect their ownership rights in the internet era, the goal of services like Napster, Gnutella, LimeWire and other related services was to offer customers the ability – albeit illegally – to enjoy 'their' digital music at any time or anywhere by converting rivalrous digital resources into non-rivalrous ones. Many of these sites, technologies and platforms were based on a central published directory, by means of which users could search for and locate files. This also presented a single point of failure for the entertainment industry to target. Indeed, following several prolonged court battles, the entertainment industry managed to shut down many of these sites and services by targeting those central network directories and 'nodes'.

However, the internet user community's response to the primary vulnerability of Napster's centralised directory structure was swift and effective: namely, the development of the peer-to-peer product and network protocol BitTorrent, a network protocol that does *not* require a centralised directory to facilitate internet file-sharing activities and, subsequently, establishes an information-sharing environment that is difficult to restrict in any meaningful way. Consequently, digital property owners remain challenged by people who draw on BitTorrent-based technologies to obtain pirated products. More recently, and without making an assessment about the quality of information conveyed, social media services such as Facebook, YouTube and Twitter (allowing individuals to broadcast their views to a wide audience) and the rise to prominence of 'alternative news organisations' (employing partisan reporters to craft preplanned narratives that cater to a given audience that previously had felt marginalised by traditional media) likewise demonstrate the emergence of influential and authoritative platforms from out of the broader networked community that challenge the status quo of power in society. As with the nature of the internet described earlier, these niche groups from outside the traditional structure of social prominence 'routed around' obstacles in responding to external challenges and perceived user needs.

This ability of a grassroots community to respond, of its own volition and expertise, to emerging needs that are not served by existing sources of community authority and influence can generate potential conflicts over questions of power, authority and/or legitimacy in society – along with revealing new and evolving social norms and expectations regarding the use of technology by individuals.

As evidenced in both the PGP and BitTorrent examples, the law traditionally, and often significantly, lags behind technological development and, as Arquilla and Ronfeldt (1997) note, sometimes 'it takes a network to fight a network'. In other words, when one internet user or entity attempts to exert control over information through the application of assorted technical or political methods of restricting information exchange (such as through DRM or legislative/regulatory controls), other internet users may respond against such efforts by inventing new methods to enable that information exchange. The process tends to be cyclical in nature: for nearly every attempt made to constrain information exchanges, equal and opposing attempts are made to enable them. In describing this phenomenon as regards the dialectic of control in social systems, Giddens (1984) writes that such a cyclical dynamic is a constant and that ideas of 'power' within these social systems are the capacity of any of the conflicting entities to 'achieve outcomes' beneficial to their respective goals. In terms of DRM, when a given protection scheme is broken by third parties, a new one is introduced; it too is assessed and probably breached, and the cycle then repeats itself. Throughout this process, both 'networks' maintain some semblance of power – either *de facto* or *de jure* – or, sometimes, a shifting combination of both.

These are two examples of how technology capabilities can influence political realities in society and disrupt existing or traditional sources of power and authority held by both government and commercial entities. But these are certainly not the only examples. The US government did not 'own' the rights to the public nature of the mathematics (that is, the mathematical algorithms) of PGP but had legal authority to control its public distribution in the name of the 'public interest' and under the rubric of protecting national security. However, that authority was challenged by those

distributing that information over the internet, who believed that it was also in the public interest to have digital communications protected from government eavesdropping. Napster and subsequent concerns over DRM show how digital information can be distributed and used in ways not approved by its legal owner; they also demonstrate both the evolving perceptions of internet users about using technology and how the community can develop solutions to uncatered-for marketplace or user needs. Of course, in each example, the same outcomes might have been achieved without use of the internet or other 'cyber' technologies or capabilities, though not with the speed and ease which these resources offer.

Nevertheless, despite the potential for networks to score these victories against the traditional paradigms of power and control, we must remember what we said earlier about their potential also to simply replicate the age-old balance of power. In other words, the internet offers radical new resources to both sides, but crucially, *it does not change the sides and their ultimate goals*.

## Conclusion

What does the internet have to do with political realism?

In their discussion of the internet as a weapon in what they call 'network-centric warfare', Cebrowski and Garstka (1998) believed that the internet and its related technologies are the result of the co-evolution of economics, information technology and business processes, thereby representing a fundamental, disruptive change to the contemporary social fabric and its communications mechanisms. Although drawn from a military and national security perspective, the three elements espoused by Cebrowski and Garstka can now be transposed, or expanded, here into a description of the major impacts made upon social communication by the internet in the Western world, specifically:

- the shift in focus from the platform to *the network*
- the shift from viewing network participants as independent to viewing them as part of a *continuously adapting ecosystem*
- the importance of making strategic choices to *adapt or even survive* in such changing ecosystems.

Within networked environments, information exists in a nuanced and dynamic state, based upon how it may be exchanged (or flow). At times, this dynamic can enable networked entities (or individuals) to route information flows around assorted obstacles and allow information to be exchanged without the permission of its owner (such as the global distribution of PGP despite US government laws, or BitTorrent). And yet at other times, it may allow an information owner to exert new and potentially significant controls over those flows (such as new forms of attempted DRM on digital products).

Networked technologies can both enable and constrain flows of information and knowledge Since the mid-1990s, the political reality of 'cyber' and the nature of internet technologies continue to demonstrate that these conflicts – both technical and political – are not easily addressed by any one entity or special interest. As observed by

Czerwinski (1996), at the same time as the world began embracing internet technologies during the 1990s, network-based systems evolved rapidly into a loosely coupled yet complex system – meaning that the new and chaotic behaviours of 'networked life' in turn generated their own new expectations of what should and should not be allowed. Today, it is clear how this has also resulted in a radical change to the concept of 'society' itself: that is to say, 'society' is fast becoming a globalised notion, synonymous with the borderless reach of the internet itself. For individuals, corporate leaders and political authorities hitherto comfortable with centralised hierarchies of command and control – with top-down executive fiat and state-based sovereignty – this new situation is threatening to change the very idea of the 'powers that be'. Or perhaps not. As I have suggested throughout, despite the language of 'sea-change' and 'paradigm-shift' that the internet encourages, there is an argument that the entire phenomenon is still unfolding squarely within the traditional scheme of human life: that is to say, we still find that we are using the old language of 'power', 'authority', 'control', 'security', 'rights' and so on to describe the new reality. This would suggest that the internet owes its very success to its basic function of reproducing in bold new ways the unchanging dynamics of human nature in politics and international relations: that is, dynamics that were postulated (and feared) by classical realists such as Reinhold Niebuhr (1932) and Hans Morgenthau (1948). Whether it will, or could actually, go on to rewrite those dynamics is something that we will have to wait to see.

## Bibliography


Abbate, J. (1999), *Inventing the Internet*, Cambridge, MA: MIT Press.

Arquilla, J. and D. Ronfeldt (1997), 'The advent of netwar', in J. Arquilla and D. Ronfeldt (eds), *In Athena's Camp*, Santa Monica: RAND Corporation, pp. 271–93.

Arquilla, J. and D. Ronfeldt (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica: RAND Corporation.

Arthur, C. (2009), 'The Streisand effect: Secrecy in the digital age', *The Guardian*., 19 March.

Card, A. (2002), 'Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security' [Memorandum], available at <http://www.fas.org/sgp/bush/wh031902.html> (last accessed 15 June 2018).

Castells, M. (1983), 'Crisis, planning, and the quality of life: Managing the new historical relationships between space and society', *Society and Space*, vol. 1, no. 1, pp. 3–21.

Castells, M. (2000), *The Rise of the Network Society; The Information Age: Economy, Society, and Culture*, Cambridge, MA: Wiley-Blackwell.

Cebrowski, A. and J. Garstka (1998), 'Network-centric warfare: Its origin and future', *US Naval Institute Proceedings*, vol. 124, no. 1.

Czerwinski, T. (1996), 'Command and control at the crossroads', *Parameters*, Autumn, pp. 121–32.

Dyer-Witheford, N. (1999), *Cyber-Marx: Cycles and Circuits of Struggle in High Technology Capitalism*, Chicago: University of Illinois Press.

Giddens, A. (1984), *The Constitution of Society*, Berkeley: University of California Press.

Leiner, B., V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts and S. Wolff (2003), *A Brief History of the Internet v.3.32* (revised 10 December), The Internet Society, available at <http://www.isoc.org/internet/history/brief.shtml> (last accessed 15 June 2018).

Moody, G. (2017), 'Thai Government Forbids any Online Contact with Three Overseas Critics of the Monarchy', *TechDirt*, available at <https://www.techdirt.com/articles/20170413/09283537140/thai-government-forbids-any-online-contact-with-three-overseas-critics-monarchy.shtml> (last accessed 15 June 2018).

Morgenthau, Hans J. (1967) [1948], *Politics among Nations*, 4th edn, New York: Knopf.
Niebuhr, Reinhold (1932), *Moral Man and Immoral Society*, London: Westminster John Knox.
Polanyi, K. (1966), *The Tacit Dimension*, New York: Doubleday.
Rose, N. (1999), *Powers of Freedom: Reframing Political Thought*, Cambridge: Cambridge University Press.
Ryle, G. (1946), 'Knowing how and knowing that', *Proceedings of the Aristotelian Society*, no. 46, pp. 1–16.
Urry, John (2004), 'The "system" of automobility', *Theory, Culture and Society*, vol. 21, nos 4–5, pp. 25–39.
Zimmerman, P. (1996), 'Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation', available at <https://philzimmermann.com/EN/testimony/index.html> (last accessed 15 June 2018).