The projection and measurement of cyberpower

Venables, A. , Shaikh, S.A. and Shuttleworth, J.

Original citation & hyperlink:
Venables, A. , Shaikh, S.A. and Shuttleworth, J. (2015) The projection and measurement of cyberpower. Security Journal, volume 30, no. 3, pp. 1000-1011
http://dx.doi.org/10.1057/sj.2015.35

DOI 10.1057/sj.2015.35
ISSN 0955-1662
ESSN 1743-4645

Publisher: Springer

Original Article

The projection and measurement of cyberpower

Adrian Venables*, Siraj Ahmed Shaikh and James Shuttleworth
Coventry University, Coventry, CV1 5FB, UK

*Corresponding author.

Abstract Cyberspace and cyberpower are terms that are increasingly used in common parlance, but are notoriously difficult to define and measure. This article builds on previous work defining the properties of cyberspace in terms of vertical layers, which when combined with a representation of distance presents a three-dimensional model. The unique attributes of cyberspace can be harnessed for power projection, the aim of which is ultimately to alter the behaviour of individuals. Although cyberspace has yet to be used as a medium to demonstrate conventional hard power of coercion and threats supported by physical force, it does present a suitable medium for the projection of soft power of attraction and imitation. These are defined within the context of the online environment and by drawing on the techniques used to optimise Web-based commerce, potential methods of implementing and measuring the success of a campaign of cyberpower projection are proposed.
Security Journal advance online publication, 2 November 2015; doi:10.1057/sj.2015.35

Keywords: cyberpower; soft power; social media; e-commerce; measures of effectiveness

Power and Cyberpower

According to Dahl (1957), the aim of a campaign to project power and influence is to affect the behaviour of people such that A can be regarded as having power over B to the extent that he can get B to do something that B would not otherwise do. This was expanded on by Nye (2010), who in noting that the concepts are elusive to define and measure, describes their aim as being to affect the behaviour of an individual to act in a way that they would not otherwise do, to shape the preferences of others by determining their wants or by setting agendas through external actions or persuasion. This power can be targeted as precisely as to a single individual or small group, such as the European Union sanctions against the leadership in Zimbabwe (BBC News, 2002) or to an entire population as exemplified by radio propaganda broadcasts during the Second World War (Concho, 2004).

Traditionally a state's national power was considered to be dependent upon factors such as geography, national resources, population size or wealth as these were regarded as the constituent elements required for the creation of military power (Tellis *et al*, 2000). The ability of a nation to be able to protect its own borders from attack while demonstrably

threatening a neighbour was seen as the ultimate symbol of national strength. In the post-industrial age, definitions of national power began to introduce the notion of a knowledge revolution that foreshadowed the growth in importance of the role of information technology and innovation in society. However, Tellis *et al* (2000) comments that these were ultimately seen as contributory factors in the generation of a country's financial wealth that could be converted into military capability if needed.

The emergence of cyberspace and the concept of cyberpower require an evaluation of the definition of how power and influence can be projected in an interconnected world. As cyberspace has no physical boundaries, nations do not have territory to protect or ways to threaten a neighbour's borders and natural resources using the conventional definitions of power projection. Therefore new ways are needed to be able to define power in order to be able to use the medium to influence and shape the behaviour of others. Defining cyberspace has attracted much debate, particularly for the military, which is keen to emphasise its uniqueness to attract new funding in order to explore the opportunities it has to offer. The UK Ministry of Defence's Development, Concepts and Doctrine Centre (2013) and US Department of Defence (2007) provide similar descriptions emphasising its interdependence on a range of constituent elements such as networks, computer systems and embedded controllers. A different approach is however proposed by Sheldon (2011), who defines cyberspace in terms of four vertical layers, which are described as follows with proposed indices of how they can be measured.

Infrastructure layer: The physical aspects of cyberspace, which incorporates computer hardware, servers, networking components, cabling, satellites and other dedicated facilities. This also includes those devices that users interact with, such as PCs, laptops, tablets and smart phones. This layer could be measured by the proportion of the population with access to the Internet, average time between users upgrading hardware, levels of smart phone ownership, the number of Internet Service Providers (ISPs) relative to the population and the number of international gateways providing global connectivity.

Physical layer: Features that are governed by physics and comprise the properties associated with the transfer of data across the infrastructure layer. These include the characteristics of the electromagnetic spectrum such as the passage of photons in fibre-optic cables, electrons in cablings and wireless propagation from short-range Bluetooth communication to international satellite links. Measurements of this layer could incorporate the proportion of the nation served by copper cable compared with high-speed fibre-optic cable, number of Wi-Fi hotspots per head of population, mobile phone coverage, average data consumption per subscriber and the cost of access compared with average national salary.

Syntactic layer: The manner in which data is formatted to facilitate communication between and within components of the infrastructure layer. This includes communication protocols, software components and network routing algorithms. Measurements could include the level of encryption routinely employed, the proportion of computers protected by anti-virus and the levels of infected machines, degree of network prioritisation (Net neutrality) and the number of Domain name registrations.

Semantic layer: This component enables human users to make sense of the information and for it to become useful to them. This includes elements such as the type and popularity of user interfaces, application software, as well as the linguistic, cultural and human factor

considerations employed in their design. Measurement indices include the proportion of gross domestic product from online business, percentage of web pages produced in the indigenous language, percentage of population who are active social network users, levels of cybercrime and the amount and effectiveness of legislation and enforcement.

To this four-layer model of cyberspace, we add an additional human element as we consider it fundamental to the nature and understanding of cyberspace and cyberpower. This is because the domain is dependent upon man and, unlike the other environments with which it is often compared, land, sea, air and space, it requires human intervention for its creation, maintenance, exploitation and ultimately its destruction. Furthermore, the interpretation of the semantic layer, which provides information that is useful and understandable to human operators, has to be variously tailored to suit the needs of the end user and will need to accommodate factors such as language and culture. This has been recognised with the development of human–computer interaction as a multidisciplinary field in which psychology and other social sciences unite with computer science and related technical fields with the goal of making computing systems that are both useful and usable.

When viewed in this context cyberpower can be described in terms of the level of control of these layers, noting that power over one does not result in governance of all. The ability to quantitatively measure a range of variables within each layer could be used to produce a comparative index of power. These could then enable a relative position against an economic competitor or military adversary to be calculated. Specific areas that are shown to be comparatively weak can then provide an indication of where effort needs to be concentrated to improve performance.

In addition to defining cyberspace in terms of vertical layers, it can also be considered horizontally in terms of Near, Mid and Far geographic operating space. These are described in Table 1 and are based on those defined in the UK Ministry of Defence's 'Cyber Primer' (MoD, 2013a, b). Control of the local Near space is vital to protect national or local interests and through the 'no man's land' of Mid space, power is projected into Far space, which will be the Near space of a target country or competitor. An analysis of an adversary's strengths and weaknesses in each of these three areas can provide information on possible attack vectors that can be utilised to reduce their influence and ability to operate freely in cyberspace.

In combining these five layers with the concepts of Near, Mid and Far space, cyberspace can be redefined in three dimensions as shown in Figure 1. This can be used to illustrate that although cyberpower may be exercised in some elements of the domain, it does not guarantee control of all, and that some techniques targeting a particular aspect may only have a limited overall effect against an adversary. This model also enables attacks to be

Table 1: The three horizontal layers of cyberspace

Environment	*Description*
Near space	Local networks and systems that are considered vital to support critical national infrastructure and services and are assumed to be controlled and protected by national or governmental agencies
Mid space	Networks and systems critical to access global cyberspace but over which there is no local control or protection. Typically these may be geographically distant and owned by a foreign commercial company or a third party state
Far space	Networks and systems that form a competitor or adversary's near space and which must be influenced or controlled as part of a campaign to project power and influence through cyberspace

appreciated in terms of their intended areas of effect and for the defender an appreciation of where the greatest risk to their organisation lies.

To demonstrate how our model of cyberspace can be applied in practice, Table 2 illustrates how each component can be defined in terms of a national government's attempt through the use of video clips on social media to influence European-born Jihadists who have travelled to the Middle East to return to the West. In this case the targets have been identified as predominantly using mobile telephony and are active on a variety of social media platforms. Of note is the inclusion of anonymous hacktivists operating in Mid Space who have been active in the disruption of extremist media platforms through their #OPIsis campaign (Sullivan, 2015).

The Development of Soft Power in Cyberspace

Control of the vertical and horizontal layers of cyberspace described above is fundamental to enable power and influence to be exerted. This can be directed both inwards towards a local target population in Near space as well as to a target in Far space. The ability to effectively

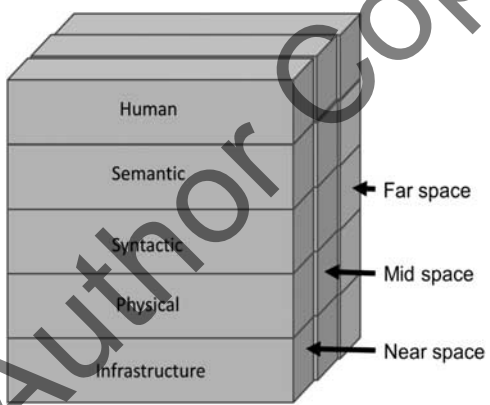

Figure 1: Three-dimensional model of cyberspace.

Table 2: Illustrative components of cyberspace

	Near space	*Mid space*	*Far space*
Human	Government Employee	'Anonymous' Hacktivist	Jihadist
Semantic	Video production Software	Routing software	Social media application
Syntactic	MPEG-4 video format	Transmission Control Protocol (TCP)/ Internet Protocol (IP)	MPEG-4 video format
Physical	Electrons in Ethernet cable and light in fibre-optic cable	Light in fibre-optic cable and radio frequency communication within satellite and microwave links	Radio frequency communication within mobile telephone networks
Infrastructure	Video production suite, desktop computer and Local Area Network	Microwave and satellite link, fibre-optic undersea cable and ISP infrastructure	Mobile telephone network and smart phone

translate cyberpower into an effect in the physical domain requires a clear understanding of what objectives are desired and how success or failure can be determined. Any cyber strategy must be fully coherent with the wider policy aims of the physical world as cyberspace and cyberpower do not exist in isolation and any actions must be part of a wider political objective and campaign plan.

Projecting power through cyberspace differs from that of the traditional concept of military 'hard' power, which seeks to change behaviour through direct inducements of threats and coercion (Nye, 2010). Although methods of measuring the potential effectiveness of conventional military forces based on their known or estimated capability are well established, to date there has not been a fully attributed nation on nation cyber attack (Rid, 2012). This has led analysts to only be able to speculate on a country's capabilities and how a cyber conflict may unfold and what effects may be achieved. However, several countries have already stated that they are engaged in the militarisation of cyberspace, indicating that they are preparing to be able to engage in offensive cyber operations, which may act as a credible deterrent to future attacks. The UK Ministry of Defence (2013a, b) has announced its intention to build a counter-attack capability and China has reportedly had cyber warfare units since 2003 with the US Cyber Command achieving an initial operating capability in 2013 (Nato, 2009).

An alternative to the methods of military hard power to achieve national objectives is to adopt the concept of soft power developed by Nye (1991). Soft power targets human factors and aims to 'get others to want the outcomes that you want' through the power of attraction, which includes non-material means such as culture, political values and foreign policies (Treverton and Jones, 2000). After a decade of military operations in the Middle East, which it may be argued has produced unclear outcomes, the benefits of soft power as the policy of attraction over coercion are seen as offering an alternative means to achieve national objectives. According to Nye (2004), the countries that are most likely to gain soft power should display the following three attributes to optimise their attraction on the global stage:

- Their dominant culture and ideas should align to the prevailing global norms, which include liberalism, pluralism and autonomy. This sets the standard to which other countries might seek to attain, including a structure that enables free debate and an active engagement across a range of diverse topics with individuals able to make informed, un-coerced decisions. However, these can be viewed as being very much western ideals and it can be argued that to gain soft power in countries without these traditions or ambitions it is necessary instead to meet local norms that the target population may be familiar with and aspire to.
- Second, to be able to effectively disseminate the desired message it is necessary to have access to multiple channels of communication to enable influence to be exerted over a wide range of media. To provide a coherent message, this must be available through the entire range of media types that the target has access to.
- Finally, for a country to gain soft power, it must be seen to be credible in terms of its domestic and international performance so as to be attractive to the target it wishes to influence. This requires the influencing country to be highly regarded, trustworthy and be seen to have a good reputation on the world state in terms of its national values and behaviour.

Further research by Kroenig *et al* (2010) into the concept of soft power suggests that to be successful, states must communicate to their intended targets in a 'functioning market place of ideas' where there is a competition of messages free from state influence. This would

include such forces and mechanisms as censorship and propaganda. In addition, they propose that the target must be potentially receptive to the message, which must be credible, attractive, repeated and contain emotional content. It must therefore be a carefully tailored campaign directed at those who are amenable to the message and be able to influence decision makers. However, as noted by Hall and Smith (2013), soft power cannot compensate for what may be regarded as other unattractive national policies as has been seen in China, where despite a substantial investment in soft power projection, evidence has been used to demonstrate that it has had little or no positive effect on how the country is perceived by its neighbours.

The role of soft power in the projection of the UK's national power was recognised in 2013 by the appointment of a House of Lords Committee to determine how it could be deployed in the national interest. The ability of cyberspace to reach large numbers of people was highlighted in the report by the rise in urbanisation leading to large concentrations of people in relatively small areas becoming intimately connected by electronic means and more aware of 24-hour broadcasting and social media (House of Lords, 2014a). The impact of this was highlighted by Fuchs (2012) in the role of BlackBerry Messenger and Twitter in the 2011 London riots, with both the Prime Minister and Home Secretary making particular reference to their role in organising the disturbances and countering the Police reaction. The link between rolling news services and social media was also more recently exemplified by Whitehead and Evans (2014) when a Qatari airliner was subject to a hoax bomb threat. Although the passengers were not told of the situation, it was broadcast on national news and subsequently on Twitter, which was being monitored by those on board. It is significant that in this potentially dangerous situation, those most affected were not being informed of events by the flight crew, but by journalists and members of the public on the ground.

Although soft power is clearly an attractive concept, the battle for hearts and minds in a cooperative framework only works when the target is amenable to the message. Examples in which it has failed include Kuwait in 1991 when only decisive military force was effective and it has been noted by Greenwald (2010) as so far having a negligible effect on Islamic militants in the Middle East. Using the example of Russian activity in Georgia and Ukraine he noted that it also has a tendency to fail when the target is able to either block or effectively counter the message with its own information campaign. Furthermore, once it becomes clear that there is no plan to recourse to hard power, either economic or military, a policy that relies on soft power alone will fail, with the result that an adversary will take advantage of a lack of a credible military threat for their own ends.

These limitations of deploying soft power alone were recognised by Nye (2009) in the development of the concept of smart power, which is the combination of hard power coercion and payment with the soft power attributes of persuasion and attraction – the use of carrot and stick, which to be most effective should be mutually reinforcing. Thus the effective use of technology and information combined with conventional military power can act as a force enabler so long as their strengths and limitations are well understood.

Projecting Power in Cyberspace

Although conventional military hard power that results in direct destruction and harm through cyberspace has yet to be demonstrated, the use of intimidation and coercion to exert

power has been ably demonstrated by the Islamic State in Iraq and the Levant (ISIL) through its media campaign (Lister, 2014). Directly in contravention of the traditional theory of soft power's attraction and appeal to wider cultural norms, their prominent videos of beheadings and the promotion of an extremist ideology have been widely disseminated. By broadcasting news of their latest atrocity around the world through multiple channels, including the Internet, their message has been further disseminated through social media and blogs. This effectively increases their exposure beyond their initial audience, with the opportunity to reach future potential converts to their cause. Images censored by traditional media are readily available online in their original format and may be seen to play a role in effectively inspiring the radicalised at home and abroad, while demonstrating the consequences of dissent to those already living under its regime. The quantity of images published online may also act to normalise these acts of terror, desensitising potential perpetrators from considering these actions abnormal and extreme.

Although the longer-term impact of ISIL's campaign of hard power in cyberspace has yet to be fully analysed, there are already examples of how effective a soft power campaign can be on a receptive audience that is technologically literate and with a wide individual ownership of devices capable of receiving the message. Barak Obama's use of social media as a tool of soft power proved particularly noteworthy in the 2008 presidential campaign. In the previous 10 years US broadband Internet access had doubled to 55 per cent and social networking technologies had matured, technology which Obama's team fully exploited and placed at the centre of their strategy. Although all the candidates hoping for the Democratic party nomination had websites, he made better use of Twitter, text messages and Facebook to proactively engage with his supporters in publicising his message, gaining supporters and fund raising (Talbot, 2008).

At an international level, the House of Lords' committee on soft power noted that a country's cultural reputation is seen as being an important element in the projection of power and influence, with the role of national broadcasters particularly emphasised. In this respect the British Broadcasting Corporation (BBC) was seen as a unique strength for the United Kingdom predominantly due to its perceived independence from the Government, its international services and the dominance of the English language worldwide (House of Lords, 2014a). In particular, during his evidence to the committee, Nye stated that in an information age soft power relies on communication and that it was not just whose army wins, but also whose story wins that matters in exercising power (House of Lords, 2014b). However, the power of the message may be lost if it is seen as promoting a specific national message and the committee concluded that fundamental to gaining the trust of others and promoting a sympathetic view of the United Kingdom is to promote characteristics that have broad appeal. These must have attributes that are intrinsically linked to the United Kingdom, yet are seen to be independent of government interference. Evidence of the power of the BBC was noted by the committee in their final report by making specific reference to the alleged jamming by the Iranian authorities of the satellite signal broadcasting its content (House of Lords, 2014a).

An integral component of any campaign to influence behaviour is an understanding by the target of the originator and their intentions. This may be clear when faced with military force or a radio broadcast announcing its origin, but may be erroneous if it is part of a deception plan. However, as Rid (2011) notes, quoting Clausewitz's statement as war being an extension of politics, attribution will always follow at some point in a conflict. Within

cyberspace though, attribution may not be straightforward and misinformation is rife. Social media in particular has been noted as providing an environment in which individuals have been deceived, sometimes with devastating personal consequences (Tsikerdekis and Zeadally, 2014). Established media organisations and democratic governments with an online presence strive to ensure the credibility of all information that they broadcast and that it is not perceived as state-sponsored propaganda. To achieve this, it must be truthful and open to corroboration, clearly attributable to the source and sensitive to local cultures and religions (Nye, 2008). However, despite the efforts of reputable news organisations to disseminate information, which to the best of their knowledge is unbiased and neutral, the mass of conflicting information online can be problematic. Bastardi *et al* (2011) illustrated that what people believed to be true and what they wish to be true can be very different with people evaluating evidence in a biased manner. Examples demonstrated that where political convictions are challenged by scientific studies, people derogate from the methodology used or interpret the results differently to fit their preconceived beliefs.

In order to be able to influence a target audience, it is necessary to have not only a compelling message, but also access to the target's network infrastructure for its dissemination. As noted by the OpenNet Initiative (ONI), which seeks to identify and document Internet filtering and surveillance, network resilience is becoming an increasingly important factor (opennet.net, 2014). In particular, the ONI notes that the content of social media applications has attracted the attention of governments around the world and some have sought to block selected elements of the sites or even shut off access entirely to those that contain politically or socially sensitive content. An understanding of both the level of censorship a target audience is subject to and their awareness of methods such as proxies to circumvent them are an important aspect in any attempt to project power through cyberspace.

Measuring the Effect of Cyberpower

Because of the inconsistency in how people interpret information and the potential bias in how it may be understood, the House of Lords committee (2014a) echoed Nye (2010) in noting that soft power cannot be applied instantaneously, but that it is a long-term activity that must be carefully planned and implemented (House of Lords, 2014a). Influence and affinity cannot be easily quantified and attempts to do so may result in measuring only those aspects that can be more easily identified as discrete variables and not the more abstract elements such as the effect of the message. Some matrices can be identified however, such as those used in Obama's successful Presidential election campaign, which were measured not only in terms of monetary donations, but also through comparing the numbers of Twitter followers of each candidate, which provided a direct indication of relative popularity as did MySpace 'friends' and Facebook supporters (Talbot, 2008). Trends in web traffic and Internet searches also provided indicators as to how the campaign was progressing towards the all-important primaries. In addition to purely just measuring the number of followers in Twitter, other methods have been used to determine the spread and impact of a message. Research by Cha *et al* (2010) has shown that the use of hashtags that identify certain topics as well as mentions and retweets can provide a more reliable indication of the influence of the originator than comparing just the number of followers.

The use of social media in which users actively interact with the application by posting their own messages and engaging with others' readily lends itself to quantitative analysis. However, methods also exist to measure user engagement with other methods of communication such as websites in which there may be no direct data input. Many of the techniques that can be applied to the measurement of a soft power message can be taken from the domain of Internet commerce in which website visits are recorded and analysed with the aim of optimising the user experience and increasing sales. Google analytics is a facility that provides information about a website's traffic and measures the number of visits that results in actual sales. It can record in real time for later analysis how and from where the user accessed the site, such as from search engines or social media, and tracks their interaction with the pages while logging what material is downloaded (Google Analytics, 2014). Since July 2014, Twitter has also provided a powerful facility to investigate the use of its platform with its own analytics function that allows users to discover who has viewed their Tweets and provides an overview of their profiles (Twitter Analytics, 2014). Also commonly used by websites to aid their analysis of user activity is the use of 'cookies', which are small non-executable, harmless text files, downloaded by web servers onto the devices accessing their websites. These can then be used to provide user identification of the machine, record revisits, track browsing habits and tailor the user experience accordingly. By measuring the number of visits and tracking browsing habits within the site, ongoing and repeat interest in its contents can then be gauged (Jegatheesan, 2013).

Although both widely used, Google analytics and cookies do require the acquiescence of the user in allowing the use of scripting languages embedded in the websites to be executed by their browser and permitting cookies to be downloaded. An alternative method, which is purely server based, utilises monitoring software that tracks the mouse clicks and information requests of visitors to a website (Kent *et al*, 2011). This records which pages have been most accessed, what type of information is of most interest and the path that users take as they navigate its pages and the time spent on each one. Web analytics software places no information onto the visitors' computers and no personal information is collected. It is becoming regarded as an essential component of those with a commercial web presence, and although designed and primarily used as a method of optimising the web experience of potential customers, it has a potential use as a means of measuring the reaction to material designed to spread a soft power message.

In addition to the methods used in optimising online commerce, there are also other means available that could theoretically be used to project and measure the spread of soft power. These originate from techniques used by the creators of malware and involve activities that could be regarded as straying into the realm hard power and would have significant legal and ethical constraints in their use. These draw on the methods used by *botnets* to deliberately infect a target computer with executable code, which would then report back to a command and control server. This could be achieved by the victim clicking on a link within a website to download the code, or even by conducting a 'drive-by' attack by just visiting a specifically designed page containing the malware using a browser configured to grant access to scripting languages (Barwinski, 2005). This spyware's role could be as simple as reporting usage such as sites visited and material downloaded, but it could also be used for a range of other activities more commonly associated with malware, such as harvesting user credentials and directing users to fake

Table 3: Methods of measuring web site interaction

Tracking method	*Where hosted*	*Active or passive*	*Invasive*	*Site redirection*
Google analytics	Client/server	Active	Yes	No
Cookies	Client/server	Passive	Yes	Yes
Web analytics	Server	Passive	No	No
Spyware	Client	Active	Yes	Yes

websites feeding false information or even rendering the machine itself inoperable. These different tracking methods are summarised in Table 3.

All these methods are mature technologies and their ongoing development and current use would be driven by the commercial need to understand how users interact with online commerce or, in the case of the final method, for illicit purposes. Botnets were first recorded in 1999 and have increased in complexity and sophistication to avoid detection; as a result end users may not even be aware of their existence within their computers. This may particularly be the case if their signatures are not included within the anti-virus software in use and the communication to their command and control server remain unnoticed (Gassen and Gerhards-Padilla, 2012).

The techniques used in commercial advertising to attract customers and increase revenue have distinct parallels with the desire of both state and non-state actors to influence the behaviour of a population as part of a strategy to project cyberpower. Both are intended to alter the perception of their targets in order to conduct activities to the benefit of the originator. Advertising is the ultimate in soft power – the power of attraction and imitation with coercion and deterrence being an option used by those with a culture, doctrine or religion to promote. If detected, the employment of malware to harvest information or direct users to alternate sites would be seen as a provocative act by the target and depending on the nature of the information disseminated and the political situation at the time may be seen as an aggressive or possibly even a hostile act.

Conclusion

The pursuit of power has the ultimate aim of being able to control the behaviour and actions of another, even if it is against their will. Traditionally, at the state level this has been considered in terms of hard power using coercion and force with the potential of military action the ultimate threat. However, with the application of attributed military force yet to be displayed within cyberspace, the soft power of attraction and imitation has gained interest as an alternative approach complemented by military force in the physical environment as part of a coherent smart power strategy. Using cyberspace as the means of projecting soft power involves both identifying and mapping the networks and infrastructure used to reach the intended audience as well as the creation of a culturally compelling message. In this article we have sought to describe a three-dimensional model of cyberspace that can be used to identify and contextualise all the elements that need to be controlled to enable a target to be successfully reached. In considering how soft power in cyberspace can be generated and the means by which it can be delivered, we provide a method by which an assessment can be

made of its potential success in reaching its intended audience as well as how an adversary's campaign can be interrupted.

Developing a soft power campaign is a challenging undertaking as it is requires a deep understanding of a complex environment and, to be effective, must fulfil a range of criteria, not least in that it must not be seen as state-sponsored propaganda. A key aspect of any influence activity in cyberspace is a measurement of the penetration of the message within the target audience and their response to it. Human factors play an important part as unless the message can be accessed, understood and most importantly acted upon by the final recipient of the message, the campaign will have been fruitless. By drawing on well-established and mature technology designed to legitimately measure website interaction or illicitly to develop malware we have proposed methods to measure the dissemination and response to a soft power message in a target population.

References

Barwinski, M. (2005) *Taxonomy of Spyware and Empirical Study of Network Drive-by-Downloads*. Monterey, CA: Naval Postgraduate School.

Bastardi, A., Uhlmann, E.L. and Ross, L. (2011) Wishful thinking: Belief, desire, and the motivated evaluation of scientific evidence. *Psychological Science* 22(6): 731–732.

BBC News. (2002) EU agrees Zimbabwe sanctions. 18 February, http://news.bbc.co.uk/1/hi/world/africa/1827827.stm, accessed 4 February 2015.

Cha, M., Haddadi, H., Benevenuto, F. and Gummadi, K. (2010) Measuring user influence in twitter: The million follower fallacy. *Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media*, AAAI Press, Menco Park, CA.

Concho, C. (2004) Radio propagation during World War II. http://web.stanford.edu/class/e297a/WAR%20PROPAGANDA.htm, accessed 4 February 2015.

Dahl, R. (1957) The concept of power. *Behavioral Science* 2(July): 202.

Department of Defense. (2007) *Joint Publication 1-02 Dictionary of Military and Associated Terms*.

Development, Concepts and Doctrine Centre. (2013) *Joint Doctrine Note 3/13*. Ministry of Defence, UK.

Fuchs, C. (2012) Behind the news. Social media, riots and revolutions. *Capital and Class* 19(3): 383.

Gassen, G. and Gerhards-Padilla, E. (2012) Current botnet-techniques and countermeasures. *Praxis der Informationsverarbeitung und Kommunikation* 35(1): 3–10.

Google Analytics. (2014) http://www.google.com/analytics, accessed 2 September 2014.

Greenwald, T. (2010) The soft-power fallacy. *Commentary* January.

Hall, I. and Smith, F. (2013) The struggle for soft power in Asia: Public diplomacy and regional competition. *Asian Security* 9(1): 1–18.

House of Lords Select Committee on Soft Power and the UK's Influence. (2014a) Report of Session 2013–14. *Persuasion and Power in the Modern World,* HL Paper 150, London: The Stationery Office, March, pp. 33–53.

House of Lords Select Committee on Soft Power and the UK's Influence. (2014b) Oral and Written Evidence. Report of Session 2013–14, *Persuasion and Power in the Modern World,* HL Paper 150, London: The Stationery Office, March, Vol 1. p. 122.

Jegatheesan, S. (2013) Cookies – Invading our privacy for marketing, advertising and security issues. *International Journal of Scientific and Engineering Research* 4(5): 3.

Kent, M., Carr, B., Husted, R. and Pop, R. (2011) Learning web analytics: A tool for strategic communication. *Public Relations Review* 37(5): 536–543.

Kroenig, M., McAdam, M. and Weber, S. (2010) Taking soft power seriously. *Comparative Strategy* 29(5): 412–431.

Lister, C. (2014) Profiling the Islamic state. *The Brookings Institution*, http://www.brookings.edu/~/media/Research/Files/Reports/2014/11/profiling%20islamic%20state%20lister/en_web_lister.pdf, accessed 5 February 2014.

Ministry of Defence. (2013a) *Cyber Primer*. Development, Concepts and Doctrine Centre, UK, pp. 1–22.

Ministry of Defence. (2013b) New cyber reserve unit created. 29 September, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit, accessed 5 August 2014.

NATO Parliamentary Assembly. (2009) NATO and cyber defence, http://www.nato-pa.int/default.asp?SHORTCUT=1782, accessed 5 August 2014.
Nye, Jr, J.S. (1991) *Bound to Lead: The Changing Nature of American Power*. Canada: Basic Books.
Nye, Jr, J.S. (2004) *Power in The Global Information Age*. Oxon, UK: Routledge, p. 90.
Nye, Jr, J.S. (2008) Public diplomacy and soft power. *The Annals of the American Academy of Political and Social Science* 94(1): 109.
Nye, Jr, J.S. (2009) Get smart. Combining hard and soft power. *Foreign Affairs* July/August. http://www.foreignaffairs.com/articles/65163/joseph-s-nye-jr/get-smart?page=1, accessed 3 September 2014.
Nye, Jr, J.S. (2010) Cyber power. Harvard Kennedy School, May, http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, accessed 27 October 2013, p. 2.
Open Net Initiative. (2014) https://opennet.net/, accessed 3 September 2014.
Rid, T. (2011) Cyber war will not take place. *Journal of Strategic Studies* 35(1): 6.
Rid, T. (2012) Cyber-weapons. *The RUSI Journal* 157(1): 6–13.
Sheldon, J. (2011) Deciphering cyberpower. *Strategic Studies Quarterly* (Summer): 98.
Sullivan, B. (2015) Anonymous #OPIsis attackers take down ISIS twitter accounts, http://www.techweekeurope.co.uk/security/cyberwar/anonymous-isis-hack-161671, accessed 19 February 2015.
Talbot, D. (2008) How Obama really did it. *Technology Review* Sep/Oct.
Tellis, A., Bially, J., Layne, C. and McPherson, M. (2000) *Measuring National Power in the Post Industrial Age*. Santa Monica, CA: Rand, p. 5.
Treverton, G. and Jones, S. (2000) Measuring national power, RAND national security research division, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF215.pdf, accessed 5 August 2014.
Tsikerdekis, M. and Zeadally, S. (2014) Online Deception in Social Media, Library and Information Science Faculty, Paper 12, University of Kentucky UKnowledge.
Twitter Analytics. (2014) http://www.analytics.twitter.com, accessed 2 September 2014.
Whitehead, T. and Evans, M. (2014) Passengers learn of bomb scare on twitter. *The Telegraph* 6 August.