A social cyber contract theory model for understanding national cyber strategies

Raymond Bierens[1] , Bram Klievink[1] and Jan van den Berg[1]

[1] Faculty of Technology Policy & Management, Delft University of Technology, Jaffalaan 5, 2628BX, Delft, Netherlands
r.h.bierens@tudelft.nl

Abstract. Today's increasing connectivity creates cyber risks at personal, organizational up to societal level. Societal cyber risks require mitigation by all kinds of actors where government should take the lead due to its responsibility to protect its citizens. Since no formal global governance exists, the governmental responsibility should start at the national level of every country. To achieve successful management of global cyber risks, appropriate alignment between these sovereignly developed strategies is required, which concerns a complex challenge. To create alignment, getting insight into differences between national cyber strategies, is the first step. This, in turn, requires an appropriate analysis approach that helps to identify the key differences. In this article, we introduce such an analysis approach based on social contract theory. The resulting analysis model consists of both a direct and an indirect type of social cyber contract between governments, citizens and corporations, within and between sovereign nations. To show its effectiveness, the proposed social cyber contract model is validated through an illustrated case examining various constitutional rights to privacy, their embedding in the national cyber strategies and how their differences could cause potential barriers for alignment across sovereignties.

Keywords: National Cyber Strategy, Social Contract, Privacy, Cyber Security, National Security, Cyber Risk.

1 Introduction

More and more cyberspace is becoming an unsafe global environment to operate in. Today's increasing connectivity creates cyber risks at personal, organizational up to societal level. Societal risks require mitigation by government that has the responsibility to protect its citizens. Since no formal global governance exists, man-aging cyber risks should start by accepting the sovereignty of every country in cyberspace.

Studies into national cyber security strategies between 2005 and present by CCDCOE ***(1)***, OECD ***(2)*** and UNIDIR ***(3)*** plus scientific organizations Istituto Affari Internazionali ***(4)*** and TNO ***(5)*** show that for many governments sovereignty is the basis of their national cyber security strategy as part of its constitutionally agreed responsibilities. Australia ***(6)***, Austria ***(7)***, Estonia ***(8)***, Finland ***(9)***, Germany ***(10)*** ***(11)***, Hungary

(12), Japan ***(13)***, Netherlands ***(12) (14)***, Spain ***(15)***, United Kingdom ***(16)*** and United States ***(17) (18)*** all explicitly mention sovereignty in their national cyber strategy.

To achieve successful management of global cyber risks, increased alignment is necessary between these sovereignly developed national cyber strategies. Studies by Instituto Affari Internazationali ***(4)*** and TNO ***(5)*** already confirmed the potential barriers arising by the lack of agreed definitions around cyberspace, and above all of their harmonization between national cyber strategies. Priorities for national cybersecurity strategies will vary by country. In some countries, the focus may be on protecting intellectual property, and still others may focus on improving the cybersecurity awareness of newly connected citizens ***(19)***. Some nations fear (potential) cyber-attacks by terrorists on their Critical National Infrastructure, others consider information published in cyber space by terrorists, the ability for terrorists to communicate using ICT, and the gathering of intelligence on terrorists or foreign nations as topics that belong to their national cyber security strategy ***(5)***.

Insight is the first step into identifying the actual barriers that create differences between national cyber strategies and therefore can limit the alignment between them. Using social contract theory, this article introduces a direct and indirect type of social contract between governments, citizens and corporations, within and between sovereign nations. This results in a proposed social cyber contract model that is validated through an illustrated case examining various constitutional rights to privacy and their embedding in the national cyber strategies and potential barriers across sovereignties that rise from that.

The fluid nature of security threats and global cooperation suggest the need for flexibility in governance and policy structures. However, in a democratic society, such flexibilities must also be accompanied by a commensurate level of trust and accountability to citizens ***(20)***. The balance between the needs for privacy versus national security is a typical example of that. In 2011, Casman ***(21)*** used social contract theory to demonstrate the government's obligation to provide security in lieu of privacy in the post-09/11 United States. Transparency and privacy are considered as important societal and democratic values to create an open and transparent government. Only by conceptualizing these values in this way, the nature and impact of open government can be understood, and their levels be balanced with security, safety, openness and other socially-desirable values ***(22)***. On the topic of privacy, national cyber strategies show that privacy is less common as research by Luijff ***(23)*** comparing 19 national cyber strategies shows the differences for the researched national cyber strategies of Germany, Netherlands, United Kingdom and United States.

Table 1. Luijff, Besseling & De Graaf.

Country	Privacy Protection actions
Germany	Specifically defined[1]
United Kingdom	None defined
Netherlands	Specifically defined
United States	None defined

Using social contract theory, this article introduces a direct and indirect type of social contract between governments, citizens and corporations, within and be-tween sovereign nations. This results in a proposed social cyber contract model that is validated through an illustrated case examining various constitutional rights to privacy and their embedding in the national cyber strategies and potential barriers across sovereignties that rise from that.

The first part of this article researches social contract between government and its citizens in Germany, Netherlands, United Kingdom and United States. For each of these countries, the relationships between their constitution and their national cyber strategy is the topic of privacy. The second part of this article focusses on the indirect social cyber contract which consists of two agreements: between government and corporations and between citizens and corporations. Together, these two agreements form are subsidiary to the direct social contract as written down in the Constitution. After the introduction of the direct and indirect social contract, a single integrated cyber contract analysis model is introduced and used to examine if this leads to insights into potential barriers between two spheres of sovereignties.

In its last paragraph, the article defines two preliminary conclusions regarding the added value of using the social contract theory for understanding national cyber security strategies, including the introduction of a direct and indirect social contract as part of a single social cyber contract model.

2 Why the Social Contract perspective?

In 1987 the National Regulatory Research Institute published their perspective on social contract and telecommunications regulations ***(24)***. After 09/11 the social contract Casman ***(21)*** used social contract theory to redefine the balance between privacy and national security. As of 2008, the Internet Security Alliance brought social contract theory into cyberspace ***(25) (26)***. Central in all of these publications is the role and behavior of government towards its citizens as written down in the Constitution and is executed between governments, citizens and corporations. In a democratic market-driven society citizens have the option of choice between different parties as well as corporations and

[1] Research (22) did not include 2016 German Strategy that specifically defines privacy actions

can take visible and researchable actions if they feel rebalancing of the social contract is needed. For that reason, social contract as part of the field of political science is used in this research.

As an alternative, the field of economical sciences was considered. National cyber security from an economic perspective, usually related to GDP, focusses on the economic aspects such as efficiency of national cyber strategies ***(27)***, Also the dependency on global economy leaves little individual influence for Governments and therefore providing insights into potential causes for differences and similarities of national cyber strategies.

The second alternative field of science considered is technical. Cyberspace can be defined as a network of (in)direct connected devices. Cyberspace largely operates through commercial technology and communication corporations that operate globally. Because of this, governments cannot autonomously change the technical workings of cyberspace. This disfavors the technical field as a potential cause for differences and similarities.

3 The Direct Social Cyber Contract between Government and citizens

The purpose of national security is to protect the safety of a country's secrets and its citizens ***(28)***. This includes kinetic (real) threats and digital (virtual) cyber threats. Within each sovereignty, this responsibility is written down in the constitution. Within a sovereign democratic country, the Constitution of a country is the most important legal document, and has been described as the great law before which all other laws of a society must bow. It describes the core values, roles and responsibilities that apply to all citizens and government alike. A constitution becomes effective through people's consent and willingness to abide by it. This is done through social contract, and as such, a constitution is considered to be a contract ***(29)***. A nation's constitution is therefore considered to be the most common written representation of a social contract ***(30)***. In return for receiving security, citizens fulfill their own described responsibilities to obey the law. This social contract applies to both the kinetic and the digital domain.

A good example of the applicability of the constitution are the articles on privacy. Below are the articles found in the German Constitution ("Basic Law") and the Dutch Constitution ("Grondwet").

Germany – Article 10 (Privacy of correspondence, posts and telecommunications)

1) *The privacy of correspondence, posts and telecommunications shall be inviolable.*
2) *Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federa-*

tion or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

Netherlands – Article 13 (Privacy)

1) *The privacy of correspondence shall not be violated except in the cases laid down by Act of Parliament, by order of the courts.*
2) *The privacy of the telephone and telegraph*[2] *shall not be violated except, in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.*

The United Kingdom does not have a written constitution that enshrines a right to privacy for individuals and there is no common law that provides for a general right to privacy. The UK has, however, incorporated the European Convention on Human Rights ***(31)*** into its national law, which provides for a limited right of respect towards an individual's privacy and family life. This right is embedded in the UK Government's 1998 Data Protection Act ***(32)*** which aims to "to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information."

In comparison, the United States Constitution does not explicitly include the right to privacy. However, the Supreme Court has found that the fourth amendment to the US Constitution implicitly grants a right to privacy against governmental intrusion:

1) *The right of the people to be secure in their persons, houses, papers, and effects,[a] against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*

The German and Dutch Constitution are the basis for their national cyber security strategy. The 2016 German Cyber Security Strategy ***(11)*** explicitly reflects its constitution in the following paragraph:

Secure, confidential, non-manipulative electronic communications is fundamental to the exercise of the right to a private environment, the right to privacy of the citizens.

The Dutch Cyber Security Strategy ***(14)*** also refers to its constitutional paragraph on privacy in the following paragraph:

---

[2] On April 18th, the Dutch House of Representatives ("Tweede Kamer") accepted the proposal to add digital communications to this article of its constitution

The government in an international context will also enter into a dialogue with relevant private parties and will act in a framework-developing and standards-developing fashion to protect the privacy and security of users.

By Executive Order of President Obama, a Commission on Enhancing National Cybersecurity published the following recommendations in December 2016 ***(33)***:

The next Administration should launch a national public–private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management. … An effective identity management system is foundational to managing privacy interests and relates directly to security.

Germany and Netherlands explicitly refer to privacy on an individual level resulting in a strong recommendation for encryption for their communication. However, in Germany, this encryption is unconditional and without access for anyone. In The Netherlands, uncontrolled access by its intelligence agencies has been mapped against its Constitution and is therefore not yet approved at the time of this article. The United States does not recommend encryption outside reach of its own intelligence agencies but instead recommends strong authentication but with access to both corporations and citizens by law enforcement if national security requires. However, this recommendation follows their Fourth Amendment which protects its citizens against unreasonable searches and seizures.

The Constitution can be seen as a direct social contract between two parties. Comparing four constitutions shows a relationship between the Constitutions and the national cyber strategies from each nation. The constitution, and therefore the social contract, does also apply to the digital domain. This article defines the Constitution, if applicable on the digital domain, as the direct social cyber contract. Since Constitutions differ between countries, subsequently so do their national cyber strategies and (for example) their right to (digital) privacy derived from these strategies.

4 The Indirect Social Cyber Contract between Government, Corporations and Citizens

With the emergence of private companies in general, and privatized companies that are part of critical national infrastructure in particular, a third party entered social contract theory at the beginning of the 20th century: corporations. Corporations are formed by citizens who create a new legal entity together that has its own roles and responsibilities within a country with the most common purpose to maximize profits. Within a sovereign state, the Constitution also applies to the activities executed by corporation that have their legal entity within that same sovereign state. Since their purpose of profit maximization can cause conflicts with the social contract between citizens and government, the role of sovereign states expands to ensure corporations acted within the already agreed social contract.

To provide this assurance, laws and regulations are apply specifically for corporations while taking into account other drivers such as competitive market forces between corporations and citizens. These competitive market forces are assumed to have a positive effect on the behavior of corporations. In case these drivers are limited, such as within a monopoly, the government will increase its control and strengthen its laws and regulations.

Each government has to decide how to regulate their corporations, both in critical infrastructure and non-critical infrastructure. Their options are to enforce and/or to incentivize. There are two key elements to ISA's Cyber Security Social Contract ***(25)***. ***(26)***. Firstly, cyber security is seen an enterprise-wide risk management problem which must be understood as much for its economic perspectives as for its technical issues. Secondly is that government's primary role ought to be to incentivize the investment required to implement the standards, practices, and technologies that have already been shown to be effective in improving cyber security. This became the basis for the regulation of US Corporations through the NIST Cybersecurity Framework ***(32)*** that was initiated and supported by ISA's cyber security social contract.

The German National Cyber Strategy takes the opposite approach and has decided for enforcement. Their strategy (Bundesamt fur Sicherheit in der Informationstechnik, 2011) states:

The public and the private sector must create an enhanced strategic and organizational basis for closer coordination based on intensified information sharing. To this end, cooperation established by the CIP implementation plan is systematically extended, and legal commitments to enhance the binding nature of the CIP implementation plan are examined.

The Dutch Government takes a risk-based approach, to increase the resilience of vital services and processes and work to an effective joint public-private and civil-military response, and with the help of our international partners ***(12)***.

The agreement between government and corporations are ultimately intended for execution of the agreement between government and citizens in the Constitution. Therefore, the Terms and Conditions (T&C's) agreed between corporations and citizens must be taken into consideration as well. This social contract is between a corporation and its customer, the citizen. Similar to democratic government, a citizen has the freedom of choice. In government, this choice is made during the elections, with corporations, that choice is made through market forces. If one does not like the Terms & Conditions (T&C's), and unless there is a monopoly, the freedom to select another is there. The T&C's of the corporation must, off course, comply with the Constitution of the sovereign nation its legal entity operates.

In each cyber security strategy there are specific agreements between government and corporations to ensure execution of the social contract between government and citizens. Each sovereign state selects its own method cooperation within this agreement to mitigate cyber security risks, ranging from enforcement to incentivizing its corporations. Between corporations and citizens there are also specific social contract agreements through the acceptance of T&C's. The two agreements (government – corporation, corporation – citizen) together fall under the Constitution within the sovereignty and are in this research defined as an indirect social cyber contract.

5 Integrating into a single model

The previous two paragraphs have introduced the following two social cyber contracts:

1. A *direct social cyber contract* between government and citizens that is based upon the Constitution and all cyberspace related policies that are derived from it.
2. An *indirect social cyber contract* that to ensure execution of the first by legal entities other than people that consist of two agreements:
   a. An agreement between government and corporations formalized through regulation;
   b. An agreement between citizens and corporations formalized through market forces regulating the agreed T&C's;

The social cyber contract model in Fig. 1 shows the graphical representation of these two models and how they interact within a single sovereignty.

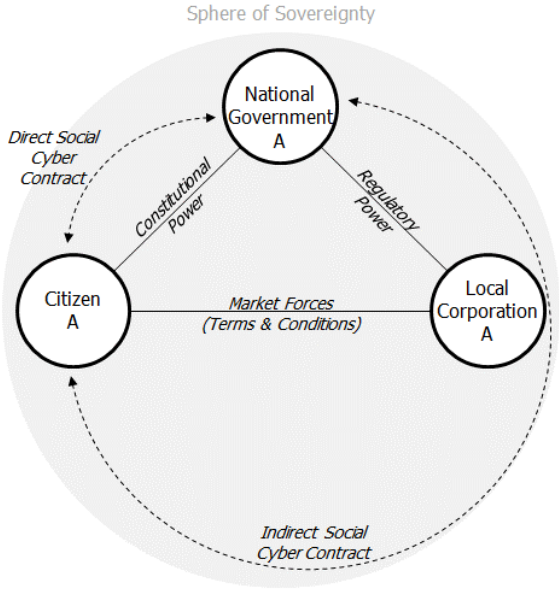

Fig. 1. The social cyber contract model.

6 Conflicting Social Cyber Contracts between spheres of sovereignty

This research focusses on the possible causes why alignment of national cyber security strategies can cause barriers to data sharing within and between sovereignties.

In order to assess if social cyber contract theory contributes to this research into possible causes, a case study on privacy has been used. Due to the lack of alignment, one would expect to see conflicts between countries where the direct social cyber contract, and subsequently also the indirect social cyber contract, are different.

Let's take two countries, A and B, where in both countries the direct and indirect social cyber contract are successfully fulfilled between citizens, government and corporations, but they are different in content. If citizen B than decides to use the service of corporation A, this citizen will have to accept the Terms & Conditions from corporation A for that specific service. However, these T&C's have been developed and executed as part of the social cyber contract fulfillment in country A.

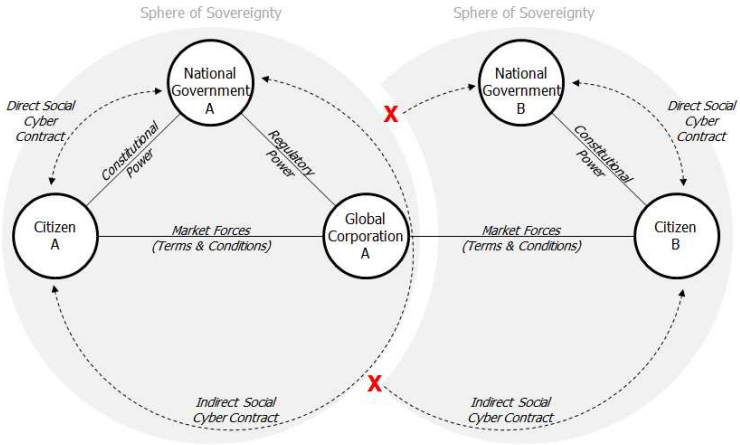

Fig. 2. Conflicting Social Cyber Contracts.

Should country B has a different social contract, this is no longer applicable. Citizen B has now, often unknowingly, become part of the indirect social cyber contract in country A. And this is only the best case. Worst case is that citizen B within country A, since he is not part of the sovereignty A, is without any legal protection at all.

In both situations, government B can no longer deliver upon its direct social contract since corporation A and government A are outside of its regulatory power. Therefore, government B can no longer fulfill his indirect social cyber contract which can have implications on the fulfillment of its direct social cyber contract between government B and citizens B.

Corporations, and especially providers of IT-driven services in global cyberspace are not limited to their own nation and often operate international across countries. The increasing interconnectedness and rapid growth of internet-connected devices only enhances this further and faster. This creates new dynamics for governments that potentially can cause tensions shown in fig 2.

The Dutch Rathenau Institute in February 2017 confirmed these new dynamics when their analysis, by request of the Dutch Senate from Parliament ("Eerste Kamer"), showed that the protection of public values is currently lacking, and there is conceptual confusion over what rules are applicable and how they should be applied ***(35)***. Sullivan & Burger ***(36)*** examine whether static and dynamic IP addresses are defined as "personal data" as defined in the new EU General Data Protection Regulation (GDPR) adopted in April 2016 and its predecessor the 1995 Directive. This would prohibit the sharing of it across countries for the purpose of cyber threat intelligence.

In May 2016 the UK's National Health Services entered into a data-sharing agreement with Google releasing 1,6 million patients medical records to Google. Applying this case to diagram 2, that would mean that Government B (NHS) would release data about citizens to Corporation A (Google), in the US. But for those citizens that also accepted the T&C's of Google, this data is now free to be analyzed since Google is allowed to use the information citizens have given them, as well as information Google gets from using their services. Even though people felt this as a clear violation of their civil rights and therefore of their social contract, legally that is more complicated since:

1. Each citizen willingly accepted the T&C's of Google before using the services;
2. The T&C's and associated data storage policies are compliant with the Constitution of the United States, being the ultimate legal entity of Google.

The NHS example also shows that when data is shared, it does not immediately violate any social contract. But when combined with other sources, it can quickly become an invasion of privacy.

7 Preliminary conclusions

The first preliminary conclusion of this ongoing research is that because since cyber risk can have societal impact, the government has an important role in executing its social contract responsibilities as defined in the constitution. Since every constitution is built upon the sovereignty of a nation, so is every national cyber security strategy. Constitutional differences, such as illustrated in this article for the topic privacy, can create differences between these cyber strategies.

The important role of private companies to maintain the internet's infrastructure, as well as providing new technology-driven IT services around the world, makes it necessary for explicitly defining their role within the social contract. The second preliminary

conclusion is that the introduction of the direct and indirect social contract provides insight on the relationship between government, citizens and corporation. Using the topic of privacy, this article shows that a single integrated social cyber contract analysis model also can identify differences between multiple sovereignties if citizens from one country start using IT services from a global country that falls under a different sovereignty.

References

1. CCDCOE (2012) *National Cyber Security Framework Manual*. NATO CCD COE Publications.
2. OECD (2012) *Cybersecurity Policy Making At A Turning Point - Analysing A New Generation Of National Cybersecurity Strategies.*, Brussels.
3. UNIDIR (2011) *Cybersecurity and Cyberwarfare.*.
4. Istituto Affari Internazionali (2011) *Ambigious Definitions In The Cyber Domain.*, Rome.
5. Luiijf, B. SdG. (2013) *Ten National Cyber Security Strategies - A Comparison.*, The Hague.
6. Ministry Of Interior (2013) *Strong And Secure - A Strategy For Australia's National Security.*, Canberra.
7. BundeskanzlerAmt Osterreich (2013) *National Cyber Security Strategy.*, Vienna.
8. Ministry of Defence (2013) *National Defence Strategy.*, Talinn.
9. Ministry of Interior (2013) *Finland's National Cyber Security Strategy.*, Helsinki.
10. Bundesamt fur Sicherheit in der Informationstechnik (2011) *Germany_BSI_2011_Cyber Security Strategy for Germany.*, Berlin.
11. Bundes Ministerium des Innern (2016) *Cyber Security Strategy for Germany.*, Berlin.
12. National Cyber Security Center (2013) *National Cyber Security Strategy.*, Prague.
13. Information Security Policy Council (2013) *Cyber Security Strategy.*, Tokyo.
14. National Cyber Security Center (2013) *National Cyber Security Strategy 2.*, The Hague.
15. Gobierno De Espana (2013) *National Cyber Security Strategy.*, Madrid.
16. HM Government (2010) *Securing Britain in an Age of Uncertainty.*, London.
17. White House (2010) *Cyberspace Policy Review.*, Washington.
18. White House (2015) *National Security Strategy.*, Washington.
19. Microsoft (2013) *Developing a National Strategy for Cybersecurity.*, Redmont.

20. John Carlo Bertot, J. SPJ. (2015) Securing the homeland in the digital age: Issues and implications for policy and governance. *Government Information Quarterly* **32**, 105–107.
21. Casman, B. (2011) *Security vs. Privacy: The Use of Social Contract Theory to Support the Government's Obligation to Provide Security in lieu of Privacy*. University of Nevada, Las Vegas.
22. Marijn Jansen, J. vdH. (2015) Big and Open Linked Data (BOLD) in government: A challenge to transparancy and privacy. *Government Information Quarterly* **32**, 363-368.
23. Luiijf, B. &dG. (2013) Nineteen national cyber security strategies. *International Journal for Critical Infrastructures,* **9**, 3-31.
24. The National Regulatory Research Center (1987) *A Perspective On Social Contract and Telecommunications Regulation.*, The National Regulatory Research Center, Columbus.
25. Internet Security Alliance (2008) *The Cyber Security Social Contract.*, Arlington.
26. Internet Security Alliance (2010) *Social Contract 2.0.*, Arlington.
27. Pascal Brangetto, M. KSA. (2015) *Economic aspects of national cyber security strategies.*, Tallinn.
28. Macmillan Dictionary (Accessed January 16, 2017) National Security Definition. In: *Macmillan Dictionary.* Available at: http://www.macmillandictionary.com/dictionary/british/national-security
29. Nyamaka, M. DM. (2011) Social Contract Theory of John Locke in the Contemporary World. In : *SelectedWorks of Daudi Mwita Nyamaka Mr*. Saint Augustine University of Tanzania.
30. American Philosophical Society (1987) The United States Constitution as Social Compact. *Proceedings of the American Philosophical Society*, 261-269.
31. European Union (1998) *European Convention for the Protection of Human Rights and Fundamental Freedoms.*, Brussels.
32. UK Government (1998) *Data Protection Act 1998.*, London.
33. Commission on Enhancing National Cybersecurity Report (2016) *Report on Securing and Growing the Digital Economy.*, Washington.
34. National Institute of Standards & Technology (Accessed February 12, 2014) NIST Cybersecurity Framework. In: *National Institute of Standards & Technology*. Available at: http://www.nist.gov/cyberframework/
35. Rathenau Instituut (2017) *Opwaarderen - Borgen van publieke waarden in de digitale samenleving.*, The Hague.
36. Burger, C. S&E. (2016) "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law & Security Review*.