CYBER SECURITY OF TOMORROW & PERSONAL DATA OF YESTERDAY

by

JAKUB HARAŠTA*

This paper aims to present new strategies of maintaining security that are powered by the (big) data. In its first part, the paper introduces the general idea of the big data analysis being used to empower security while stating obvious lack of progress in the data protection legislation. In its second part, the paper presents standard perimeter-based security and cyber security and, based on the available literature, states that it disproportionately enhances risks for computer systems. In its third part, the paper provides an overview of the intelligence-driven security, which is largely understood by the industry as the only way to maintain security facing advanced persistent threats. The last part briefly discusses possible outcome of functional separation, which protects the privacy, but renders big data for the purpose of security almost useless.

KEYWORDS

cyber security, personal data, big data, intelligence-driven security

1. INTRODUCTION

The Declaration of Independence of Cyberspace[1] written by John Perry Barlow in 1996 became, despite its obvious lack of legal force, a rather influential document and is often quoted by scholars and internet-liberalists. It sums up the general unwillingness of cyberspace to succumb to the 'weary giants of flesh and steel', as Barlow understood the world outside the cyber-

* jakub.harasta@law.muni.cz

The publication of this paper is supported by the Masaryk University - Law and Technology II project - registration no. MUNI/A/0918/2013.

[1] Barlow, J. P. 1996, 'A Declaration of the Independence of Cyberspace', viewed 22 December 2013, <https://projects.eff.org/~barlow/Declaration-Final.html>.

space and outside its immense freedom of mind. On the other hand, A Cypherpunk's manifesto[2] written in 1993 by Eric Hughes remains largely unknown and unnoticed despite its similarly interesting nature. It succeeded to precisely describe the information society we are currently living in. The basic motto of the Cypherpunk movement arose from the manifesto – *cypherpunks write code*. The Cypherpunk movement became increasingly famous when an article Crypto Rebels[3] written by Steven Levy appeared in one of the first issues of the magazine Wired. The article itself was not an astonishing piece of literature, yet it asked its audience the same question as this paper: Whether privacy will exist in the 21st century.

Cyber security is becoming increasingly important as societies have been growing dependent on critical information infrastructures, but as Adi Shamir, the co-inventor of the RSA algorithm, correctly points out, even the most secure systems can be penetrated by advanced persistent threats[4]. In fact, we have witnessed such systems to fail.[5] The general approach of various law enforcement agencies and intelligence services requiring a system administrator to implement backdoors in order to ease the acquisition of information[6] not only leads to surveillance and violation of human rights, but also to cyber insecurity. Every system, no matter how secure against the cyber threats, can be exploited. Construing backdoors in order to allow surveillance and intelligence gathering for the sake of security creates additional security risks. Therefore, a proactive cyber defence and intelligence-driven cyber security are both becoming increasingly important as well. A big data analysis, as one of the key aspects of intelligence-driven security, is what also allows ubiquitous surveillance without compromising the security by installing backdoors. Undeniably, data, information and knowledge are what fuels today's world. The privacy is going to face new challenges in massive use of big data, because the concept of big data is beneficial when facing advanced persistent threats. The privacy and data protection of yes-

---

2 Hughes, E. 1993, 'A Cypherpunk's Manifesto', viewed 22 December 2013, <http://www.activism.net/cypherpunk/manifesto.html>.

3 Levy, S. 1993, 'Crypto Rebels', Wired, vol. 1, no. 2, viewed 22 December 2013, <http://www.wired.com/wired/archive/1.02/crypto.rebels.html>.

4 Fisher, D. 2013. 'RSA Conference 2013: Experts say it's time to prepare for a post-crypto world', threatpost, viewed 22 December 2013, <http://threatpost.com/rsa-conference-2013-experts-say-its-time-prepare-post-crypto-world-022613/77565>.

5 For example Stuxnet.

6 Landau, S. E. 2010, Surveillance or Security?: the risks posed by new wiretapping technologies, MIT Press, Cambridge, Massachusetts. P. 34

terday has been struggling, unable to cope with personal data being systematically used as a resource to propel the security towards the world of tomorrow.

2. WIRE-TAPPING, SURVEILLANCE AND SECURITY

The basic assumption of cypherpunks is that someone else beside the sender and the intended receiver always consumes an unencrypted communication. This might seemed overly paranoid back then, but today with the PRISM revelation, even the greatest sceptics realised that this assumption actually might have been correct. Privacy (as a distributive right) was exploited in the past in order to strengthen security (as a non-distributive right or public good) mainly within various totalitarian regimes.[7] However, after 9/11 the discussion about the possible dichotomy of freedom and security emerged even in Western Europe and mainly in the USA itself. [8] It is an indisputable fact that collecting data and information has a huge potential to benefit security.[9] In today's globalised and interconnected world full of asymmetrical threats, this purpose is legitimate. Therefore, within this environment it is increasingly more difficult to maintain one's privacy or data integrity.

Cyber security consists of three cornerstone properties. Confidentiality, integrity and availability are forming the CIA triad.[10] This concept is insufficient to maintain high standard of security and has to be further specified by various corporate, national or international policies or by legislation. However, it is preconceptions and general understanding of the society in the centralised world what ties these tools. The post-modern nature of today's world and the evasive nature of cyberspace remain largely unreflec-

---

[7] Bobek, M., Molek, P., Šimíček, V. 2009, Komunistické právo v Československu: Kapitoly z dějin bezpráví, Masarykova univerzita, Brno. Pp. 330-363.

[8] See for example Isanga, J. M. 2009, 'Counter-Terrorism and Human Rights: The Emergence of a Rule of Customary International Law from United Nations Resolutions', Denver Journal of International Law and Policy, vol. 37, no. 2, pp. 223-255, viewed 15 June 2013, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2093414>.
Some authors suggest that this discussion was always present but due to relatively peaceful environment largely supressed. See LANDAU 2010.

[9] As evidenced by existence of various intelligence services around the world.

[10] See Graham, J., Howard, R., Olson, R. 2011, Cyber Security Essentials, CRC Press, Boca Raton.
For more security properties tied up to CIA triad see also Hsu, F. D., Marinucci, D. 2013, Advances in Cyber Security, Fordham University Press, New York. Pp. 41-42.
Alternative to CIA triad is Parkerian Hexad, see Bosworth, S., Kabay, M. E. 2002, Computer Security Handbook, John Wiley & sons, Hoboken. Pp. 116-136.

ted. New threats require new defensive mechanisms and these mechanisms require data.

When the Internet was designed, the main focus was targeted toward its functionality and not toward the security of its users.[11] Therefore, adversaries are able to exploit this mobile and anonymous environment in a manner that would have been impossible within the previous public switched telephone networks, which were largely centralised[12] and tied to a certain location. However, the need of law enforcement agencies and intelligence services to obtain some information in order to enhance the security of the society[13] did not diminish. Therefore, governments seek possibilities to embed functionalities allowing surveillance[14] in order to achieve a higher level of security. Unfortunately, the architecture of the Internet makes it quite easy to observe a user's behaviour online[15] while options to find and prosecute adversaries are relatively low. As such, the government surveillance budgets are more likely to cause harm to privacy than to uncover standalone terrorist cells.[16] The idea of intentional flaws left in the system architecture, so called backdoors, allowing law enforcement agencies, intelligence services or other groups of interest to observe an otherwise secured communication is frequently mentioned and even used.[17] On the other hand, these actions have also enhanced risks for the systems involved. Wire-tapping under legal authorisation exposes privacy for a certain amount of time and for a certain legitimate purpose. Requests for networks to be architected to accommodate authorised wiretaps expose privacy not

[11] See Baran, P. 1964, 'On distributed communication: I. Introduction to distributed communications networks', viewed 10 January 2014, <http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf>.
The original idea was to design a military network so decentralised it could work even after a nuclear strike. ARPANET evolved following this concept, despite it never were really used to military purposes.

[12] As opposite to internet which is decentralised in order for information to be possible to bypass possible network malfunctions.

[13] Through early warning or prosecution.

[14] LANDAU 2010, p. 34.

[15] Ibid. P. 139.

[16] Nagaraja, S. 2008, 'The Economics of Covert Community Detection and Hiding', viewed 8 January 2014, <http://weis2008.econinfosec.org/papers/Nagaraja.pdf>.

[17] For recent example see Paganini, P. 2014, 'French satellites sold to UAE may contain backdoored components', Security Affairs, viewed 8 January 2014, <http://securityaffairs.co/wordpress/20980/intelligence/french-satellites-backdoors.html>.

only to law enforcement agencies but also to various adversaries, therefore illegitimately.[18]

Leaving any intentional flaws in the system for the sake of surveillance not only violates the privacy of the users disproportionately, but also opens field for advanced persistent threats and therefore further compromises the system itself. Wire-tapping is often discussed only in times of high stress without a rational basis which further complicates discussion of the issue and causes an inclination towards the use of backdoors.[19] However, the distributive right of privacy is so important that any suspension of communication privacy must occur only during extreme emergency and for a brief period of time,[20] which is definitely not fulfilled in the case of permanently existing backdoors within the architecture.

To conclude, abovementioned solution is understandably unpopular because of the enhanced risks and also for the easy access to surveillance that might or might not follow the set legal standards, lawful procedures and legitimate purposes. In order to face advanced persistent threats, it needs to evolve. Today's world largely resembles the cyberspace because of the asymmetrical threats arising from groups enjoying the current human rights standards for malevolent purposes. Law enforcement and intelligence services react to this by pushing towards less stringent wire-tapping rules and even intentionally built insecurities in some systems. This tendency is also present in cyberspace when facing the advanced persistent threats by implementing intelligence-driven security.

3. INTELLIGENCE-DRIVEN SECURITY

Cyber security maintained by traditional means of protection is getting obsolete for some of the actors[21], mainly because it lingers to the idea of a perimeter that needs to be set and protected from outside threats. The idea of a

[18] LANDAU 2010, p. 247.
See also initiative Necessary & Proportionate at <https://en.necessaryandproportionate.org/text>.

[19] LANDAU, p. 247.

[20] Ibid. P. 252.

[21] Hutchins, E. M., Cloppert, M. J., Amin, R. M. 2011, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', viewed 30 December 2013, <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-Whie-Paper-Intel-Driven-Defense.pdf>.

perimeter does not suffice facing the advanced persistent threats or growing zero-day exploit market.[22]

Stuxnet, a malware targeted to affect Iran centrifuges for the uranium enrichment, is an example of such tailored advanced threat. This malware was deployed not only with the unparalleled amount of four zero-day exploits used,[23] but also with the excellent understanding of the network and the whole Natanz facility. Information sources showed that the amount of the operational uranium enrichment centrifuges significantly dropped and the production of enriched uranium stopped several times due to technical difficulties.[24] The deployment of Stuxnet was an exquisite piece of work prepared allegedly by the USA and Israel. It combined online and offline measures in order to infect computers that were protected and intentionally kept offline.[25] Whether Stuxnet was the first sophisticated cyber weapon or not is irrelevant, but it undeniably was an example of an advanced persistent threat.

Intelligence-driven security is intended to be able to keep these threats outside the system or to detect them soon enough to prevent any damage. It partially abandons the concept of a perimeter and stands on two assumptions to formulate several desirable states to be achieved.

Assumptions can be understood as following: (I) to register an intrusion takes an amount of time usually sufficient for an adversary to exploit the system and cause harm or benefit from it; (II) if the adversary is about to exploit the system, they shall sooner or later do something irregular within the system that a normally behaving user or program would not do; (III) more data means more secure networks.[26]

A perfect intelligence-driven security model using big data is able to: (I) collect data from diverse data sources both inside and outside the organisa-

[22] Stockton, P., Golabek-Goldman, M. 2013, 'Curbing the Market for Cyber Weapons', viewed 28 December 2013, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2364658>. P. 102. Also Curry, S., Kirda, E., Schwartz, E., Stewart, W. H., Yoran, A. 2013, 'Big data fuels intelligence-driven security', viewed 30 December 2013, <http://www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf>.

[23] Murchu, L. O., 2010,'Stuxnet Using Three Additional Zero-Day Vulnerabilities', viewed 15 December 2013, <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities>. Also De Falco, M. 2012, 'Stuxnet Facts Report', CCD COE, Tallinn. P. 8-10.

[24] See Albright, D., Shire, J. 2009, 'IAEA Report on Iran', viewed 9 January 2014, <http://www.isisnucleariran.org/assets/pdf/ISIS_Analysis_IAEA_Report_16Nov2009.pdf>.

[25] Bamford, J. 2013, 'The Secret War', Wired, viewed 7 December 2013, <http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/>.

[26] This assumption is not typical solely for this model. See CURRY 2013, p. 4.

tion in order to multiply the value of the information obtained; (II) use automated tools to collect diverse data types and normalize them in order to use them by analytical tools; (III) implement analytical tools capable of processing a vast amount of fast-changing data in real time to produce actionable information;[27] (IV) use advanced monitoring systems to continuously examine systems and resources and assess existing risk models; (V) actively control the deployment of counter-measures such as an additional user authentication and blocking data transmission; (VI) implement centralised warehouse of all security-related data, (VII) standardise views into indicators that are created in a machine-readable form so that they can be shared with trusted partners; (VIII) implement multiple tier infrastructure to create scalability across various vectors (geography, storage, various databases) and to process large searches; (IX) highly integrate security- and risk-management tools to facilitate detailed investigation.[28]

By using big data, cyber security can be further enhanced to be able to face new threats. This model is fit not only for the sake of cyber security, but also for the sake of security in general, which is one of the reasons why PRISM was enacted. Big data is not unknown to US government,[29] but the PRISM reached far unparalleled dimensions of sophistication and size. Intelligence-driven security in its principles was implemented in order to enhance security by a big data analysis. In fact, the PRISM had no other way to perform its function. Because of the policy of "three hops"[30], the amount of data collected reached the size of big data which is unable to be examined by traditional means.

Therefore, the use of big data can lead to more secure networks and societies. However, the data protection legislation which is currently being enacted or developed is not reflecting these policies. The most of the current

---

[27] See also Executive Office of the President. 2013, 'Report to the President: Immediate Opportunities for Strengthening the Nation's Cybersecurity', viewed 28 December 2013, Report to the president, <http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf>. P. 13-15.

[28] CURRY 2013, p. 5.

[29] See Executive Office of the President. 2012, 'Big Data Across the Federal Government', viewed 8 January 2014, <http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_fact_sheet_final_1.pdf>.

[30] See Directorate General for Internal Policies. 2013, 'The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights', viewed 22 December 2013, <http://www.fas.org/irp/eprint/eu-nsa.pdf>. P. 18.

data protection laws are based on 1980 OECD guidelines.[31] Although these were updated in 2013[32], the new guidelines plainly stated that *"the phenomenon of "big data" (…) may hold great economic and social value, but there can be privacy implications."*[33] This is barely enough for the sake of understanding big data and its impact on privacy and data protection.

4. FUNCTIONAL SEPARATION

Despite the usefulness of big data within the intelligence driven security, they pose significant risks for the protection of personal data and the right to privacy. The current legislation is largely based on concepts of notice and consent. In general, notices are largely ignored and consents are often uninformed. Yet, there are regulators clinging to these concepts.[34] The concept of choice is turning even more obsolete, because the concept of big data analytics for the purpose of security is even less understandable for the general population and largely increases the possibility of ubiquitous surveillance.[35] One of the suggested concepts to prevent the end of privacy caused by big data is the concept of functional separation.[36] The functional separation shall function as a safeguard to support regard to the individual data subjects concerned. Security of the data and all other necessary technical and organisational measures shall be implemented together with full or partial anonymisation of the aggregated data.[37] However, the functional separation does not solve the obvious tension between the perception and the reality. Lack of effective ways to share information is observed, because the data protection and privacy legislation limits the degree to which an organisation can monitor its networks for the purpose of security. Functional separation would render big data analysis for the purpose of security almost use-

---

[31] Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B. 2012, 'The challenge of 'big data' for data protection', International Data Privacy Law, vol. 2, no. 2, pp. 47-49. P. 48.

[32] OECD. 1980, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', viewed 22 December 2013, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
OECD. 2013, 'The OECD Privacy Framework', viewed 28 December 2013, <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[33] OECD 2013, p. 83.

[34] KUNER 2012, p. 48.

[35] Article 29 Data Protection Working Party. 2013, 'Opinion 03/2013 on purpose limitation', viewed 28 December 2013, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. P. 45.

[36] Ibid. P. 30.

[37] Ibid.

less, because the necessary information is often tied with a specific user account.[38]

As the security situation outside the cyberspace becomes more complicated, new dangers for the data protection emerge. I believe that given the nature of threats, we are living in the world of a permanent low-intensity ubiquitous surveillance and it is a largely inevitable fact. In cyberspace, facing the advanced persistent threats, we might soon be faced to companies implementing intelligence-driven solutions. Collecting data in order to model the standard behaviour of everyone in the system and in order to detect irregularities that might constitute possible threats might soon become standard.

5. CONCLUSIONS

This comment is not meant to provide an exhaustive solution for the incoming intelligence-driven security. It wants to introduce the intelligence-driven security to readers and provide them with an insight into possible problems with the implementation of this policy and with general data protection facing the future. I believe that the big data analysis brought the biggest challenge for the data protection and privacy so far, but at the same time, as mentioned above, it is also immensely useful in order to prevent advanced persistent threats from exploiting critical infrastructures or even societies. I argue that the low-intensity ubiquitous surveillance is extremely useful and therefore will be inevitable in the future.

REFERENCES

[1] Albright, D., Shire, J. 2009, 'IAEA Report on Iran', viewed 9 January 2014, <http://www.isisnucleariran.org/assets/pdf/ISIS_Analysis_IAEA_Report_16Nov2009.pdf>.

[2] Article 29 Data Protection Working Party. 2013, 'Opinion 03/2013 on purpose limitation', viewed 28 December 2013, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

[3] Bamford, J. 2013, 'The Secret War', Wired, viewed 7 December 2013, <http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/>.

[38] This problem is further enhanced by establishing corporate BYOD policy.

[4] Baran, P. 1964, 'On distributed communication: I. Introduction to distributed communications networks', viewed 10 January 2014, <http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf>.

[5] Barlow, J. P. 1996, 'A Declaration of the Independence of Cyberspace', viewed 22 December 2013, <https://projects.eff.org/~barlow/Declaration-Final.html>.

[6] Bobek, M., Molek, P., Šimíček, V. 2009, Komunistické právo v Československu: Kapitoly z dějin bezpráví, Masarykova univerzita, Brno.

[7] Bosworth, S., Kabay, M. E. 2002, Computer Security Handbook, John Wiley & sons, Hoboken.

[8] Curry, S., Kirda, E., Schwartz, E., Stewart, W. H., Yoran, A. 2013, 'Big data fuels intelligence-driven security', viewed 30 December 2013, <http://www.emc.com/collateral/industry-overview/big-data-fuels-intelligence-driven-security-io.pdf>. P. 5.

[9] De Falco, M. 2012, 'Stuxnet Facts Report', CCD COE, Tallinn.

[10] Directorate General for Internal Policies. 2013, 'The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights', viewed 22 December 2013, <http://www.fas.org/irp/eprint/eu-nsa.pdf>.

[11] Executive Office of the President. 2012, 'Big Data Across the Federal Government', viewed 8 January 2014, <http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_fact_sheet_final_1.pdf>.

[12] Executive Office of the President. 2013, 'Report to the President: Immediate Opportunities for Strengthening the Nation's Cybersecurity', viewed 28 December 2013, Report to the president, <http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf>. P. 13-15.

[13] Fisher, D. 2013. 'RSA Conference 2013: Experts say it's time to prepare for a post-crypto world', threatpost, viewed 22 December 2013, <http://threatpost.com/rsa-conference-2013-experts-say-its-time-prepare-post-crypto-world-022613/77565>.

[14] Graham, J., Howard, R., Olson, R. 2011, Cyber Security Essentials, CRC Press, Boca Raton.

[15] Hsu, F. D., Marinucci, D. 2013, Advances in Cyber Security, Fordham University Press, New York. Pp. 41-42.

[16] Hughes, E. 1993, 'A Cypherpunk's Manifesto', viewed 22 December 2013, <http://www.activism.net/cypherpunk/manifesto.html>.

[17] Hutchins, E. M., Cloppert, M. J., Amin, R. M. 2011, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', viewed 30 December 2013, <http://www.-lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-Whie-Paper-Intel-Driven-Defense.pdf>.

[18] Isanga, J. M. 2009, 'Counter-Terrorism and Human Rights: The Emergence of a Rule of Customary International Law from United Nations Resolutions', Denver Journal of International Law and Policy, vol. 37, no. 2, pp. 223-255, viewed 15 June 2013, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2093414>.

[19] Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B. 2012, 'The challenge of 'big data' for data protection', International Data Privacy Law, vol. 2, no. 2, pp. 47-49. P. 48.

[20] Landau, S. E. 2010, Surveillance or Security?: the risks posed by new wiretapping technologies, MIT Press, Cambridge, Massachusetts.

[21] Levy, S. 1993, 'Crypto Rebels', Wired, vol. 1, no. 2, viewed 22 December 2013, <http://www.wired.com/wired/archive/1.02/crypto.rebels.html>.

[22] Murchu, L. O., 2010,'Stuxnet Using Three Additional Zero-Day Vulnerabilities', viewed 15 December 2013, <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities>.

[23] Nagaraja, S. 2008, 'The Economics of Covert Community Detection and Hiding', viewed 8 January 2014, <http://weis2008.econinfosec.org/papers/Nagaraja.pdf>.

[24] OECD. 1980, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Pesonal Data', viewed 22 December 2013, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[25] OECD. 2013, 'The OECD Privacy Framework', viewed 28 December 2013, <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[26] Paganini, P. 2014, 'French satellites sold to UAE may contain backdoored components', Security Affairs, viewed 8 January 2014, <http://securityaffairs.co/wordpress/20980/intelligence/french-satellites-backdoors.html>.

[27] Stockton, P., Golabek-Goldman, M. 2013, 'Curbing the Market for Cyber Weapons', viewed 28 December 2013, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2364658>.