PESTEL Analysis of Hacktivism Campaign Motivations

Conference paper | First Online: 02 November 2018

pp 323–335 | Cite this conference paper

Secure IT Systems

(NordSec 2018)

Juha Nurmi & Mikko S. Niemelä

Part of the book series: Lecture Notes in Computer Science ((LNSC,volume 11252))

Included in the following conference series:
Nordic Conference on Secure IT Systems

5435 Accesses 2 Citations

Abstract

A political, economic, socio-cultural, technological, environment and legal (PESTEL) analysis is a framework or tool used to analyse and monitor the macro-environmental factors that have an impact on an organisation. The results identify threats and weaknesses which are used in a strengths, weaknesses, opportunities and threats (SWOT) analysis. In this paper the PESTEL framework was utilized to categorize hacktivism motivations for attack campaigns against certain companies, governments or industries. Our study is based on empirical evidence: of thirty-three hacktivism attack campaigns in manifesto level. Then, the targets of these campaigns were analysed and studied accordingly. As a result, we claim that connecting cyberattacks to motivations permits organizations to determine their external cyberattack risks, allowing them to perform more accurate risk-modeling.

Keywords

PESTEL analysis
Security
Online anonymity
Hacktivism
Cyberattack
Political activism
Strategic management
Risk modeling

References

1. Bakri, N.A.M., et al.: Pestle analysis on cloud computing

   Google Scholar

2. Caldwell, T.: Hacktivism goes hardcore. Netw. Secur. **5**, 12–17 (2015)

   Article Google Scholar

3. Casey, T.: Threat agent library helps identify information security risks. Intel White Paper (2007)

   Google Scholar

4. Commission, E.: Towards a general policy on the fight against cyber crime. Technical report, COM (2007) 267 final (2007). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

5. Dale, C.: The uk tour-operating industry: a competitive analysis. J. Vacation Mark. **6**(4), 357–367 (2000)

   Article Google Scholar

6. Dingledine, R., Mathewson, N., Syverson, P.: Deploying low-latency anonymity: design challenges and social factors. IEEE Secur. Privacy **5**(5), 83–87 (2007).

https://doi.org/10.1109/MSP.2007.108

Article Google Scholar

7. Gómez-Romero, J., Ruiz, M.D., Martín-Bautista, M.J.: Open data analysis for environmental scanning in security-oriented strategic analysis. In: 2016 19th International Conference on Information Fusion (FUSION), pp. 91–97. IEEE (2016)

Google Scholar

8. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Commun. ACM **46**(3), 81–85 (2003)

Article Google Scholar

9. Klein, A.G.: Vigilante media: unveiling anonymous and the hacktivist persona in the global press. Commun. Monogr. **82**(3), 379–401 (2015)

Article Google Scholar

10. Lagazio, M., Sherif, N., Cushman, M.: A multi-level approach to understanding the impact of cyber crime on the financial sector. Comput. Secur. **45**, 58–74 (2014)

Article Google Scholar

11. Nurmi, J., Niemelä, M.S.: Tor de-anonymisation techniques. In: Yan, Z., Molva, R., Mazurczyk, W., Kantola, R. (eds.) NSS 2017. LNCS, vol. 10394, pp. 657–671. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64701-2_52

Chapter Google Scholar

12. Published by BBC: Anonymous hackers ‘cost PayPal 3.5m’ (2012). http://www.bbc.com/news/uk-20449474

13. Published by Der Spiegel: State Department Secrets Revealed, How America Views the World (2010). http://www.spiegel.de/international/world/state-department-secrets-revealed-how-america-views-the-world-a-732819.html

14. Published by Der Spiegel: Visa, MasterCard Move To Choke WikiLeaks (2010). https://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/

15. Published by The Guardian: Cyber cold war is just getting started, claims Hillary Clinton (2017). https://www.theguardian.com/us-news/2017/oct/16/cyber-cold-war-is-just-getting-started-claims-hillary-clinton

16. Richardson Jr., J.V.: The library and information economy in turkmenistan. IFLA J. **32**(2), 131–139 (2006)

Article Google Scholar

17. Sheehan, N.T.: A risk-based approach to strategy execution. J. Bus. Strategy **31**(5), 25–37 (2010)

Article Google Scholar

18. Solomon, R.: Electronic protests: hacktivism as a form of protest in uganda. Comput. Law Secur. Rev. **33**(5), 718–728 (2017)

Article Google Scholar

19. Taylor, R.W., Fritsch, E.J., Liederbach, J.: Digital Crime and Digital Terrorism. Prentice Hall Press, New Jersey (2014)

Google Scholar

20. The Tor Project Foundation. https://www.torproject.org/

21. UN: United Nations Office on Drugs and Crime the SOCTA Handbook Guidance on the preparation and use of serious and organized crime threat. United Nations Office on Drugs and Crime (2010)

Google Scholar

22. Wall, D.: Crime and the Internet. Routledge, London (2003)

Book Google Scholar

23. Yar, M.: Cybercrime and Society. Sage, London (2013)

Google Scholar

24. Yüksel, İ.: Developing a multi-criteria decision making model for pestel analysis. Int. J. Bus. Manag. **7**(24), 52 (2012)

Article Google Scholar

Author information

Authors and Affiliations

Cyber Intelligence House Ltd., Singapore, Singapore

Juha Nurmi & Mikko S. Niemelä

Tampere University of Technology, Tampere, Finland

Juha Nurmi

Singapore Management University, Singapore, Singapore

Mikko S. Niemelä

Corresponding author

Correspondence to Juha Nurmi .

Editor information

Editors and Affiliations

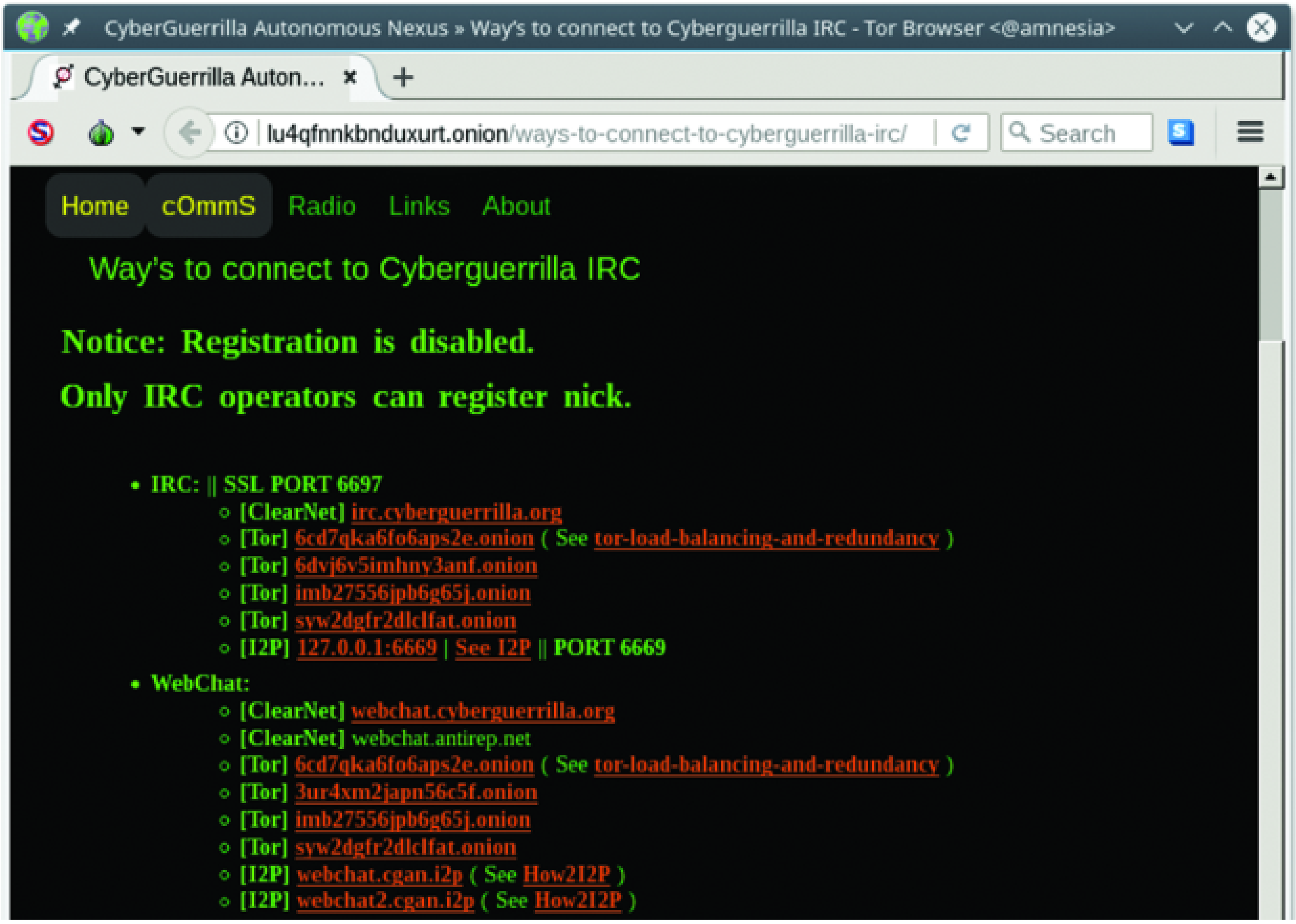
University of Oslo, Oslo, Norway

Nils Gruschka

Appendices

A Discussion Channels Within the Tor Anonymity Network are used to Coordinate DDoS Attacks

Fig. 7.


CyberGuerrilla Autonomous Nexus » Way's to connect to Cyberguerrilla IRC - Tor Browser <@amnesia>
CyberGuerrilla Auton...
lu4qfnnkbnduxurt.onion/ways-to-connect-to-cyberguerrilla-irc/
Search
Home
cOmmS
Radio
Links
About

Way's to connect to Cyberguerrilla IRC

Notice: Registration is disabled.

Only IRC operators can register nick.

- IRC: || SSL PORT 6697
  - [ClearNet] irc.cyberguerrilla.org
  - [Tor] 6cd7qka6fo6aps2e.onion (See tor-load-balancing-and-redundancy)
  - [Tor] 6dvj6v5imhny3anf.onion
  - [Tor] imb27556jpb6g65j.onion
  - [Tor] syw2dgfr2dlclfat.onion
  - [I2P] 127.0.0.1:6669 | See I2P || PORT 6669
- WebChat:
  - [ClearNet] webchat.cyberguerrilla.org
  - [ClearNet] webchat.antirep.net
  - [Tor] 6cd7qka6fo6aps2e.onion (See tor-load-balancing-and-redundancy)
  - [Tor] 3ur4xm2japn56c5f.onion
  - [Tor] imb27556jpb6g65j.onion
  - [Tor] syw2dgfr2dlclfat.onion
  - [I2P] webchat.cgan.i2p (See How2I2P)
  - [I2P] webchat2.cgan.i2p (See How2I2P)

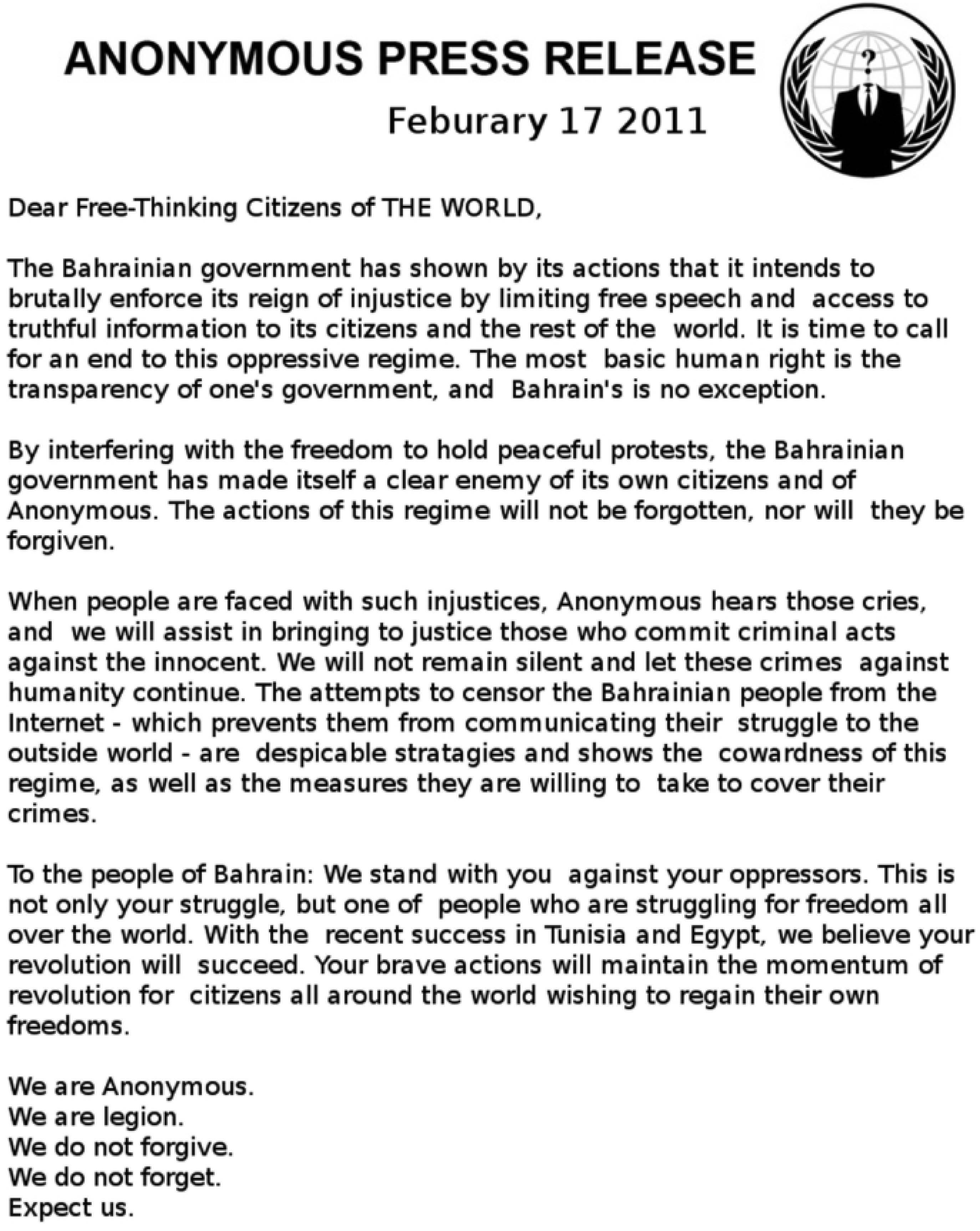
An example of anonymous onion website that shares a tutorial to connect IRC channels. These services operate inside the Tor anonymity network.

B Hacktivist Campaigns, Motivations and Targets

Table 1. An approximated timeline of hacktivist campaigns. Thirty-three cases were examined for motivation and targets. The main target sectors and countries are listed here. The number of targets refers to unique sites and online services which were attacked during the campaign. Anon. represents Anonymous, CyFi represents Cyber Fighters of Izz ad-Din al Qassam, and NWH represents New World Hackers. Please note that timeline is not clear because many campaigns failed to start or were re-launched several times. The main target sectors and countries are listed here. Finally, there are categories of motivation under the PESTEL framework. Note that several campaigns could intuitively fit under more than one category. We selected the main category.

C OpBahrain Manifesto by the Anonymous Hacktivist Group

Fig. 8.



ANONYMOUS PRESS RELEASE

Feburary 17 2011

Dear Free-Thinking Citizens of THE WORLD,

The Bahrainian government has shown by its actions that it intends to brutally enforce its reign of injustice by limiting free speech and access to truthful information to its citizens and the rest of the world. It is time to call for an end to this oppressive regime. The most basic human right is the transparency of one's government, and Bahrain's is no exception.

By interfering with the freedom to hold peaceful protests, the Bahrainian government has made itself a clear enemy of its own citizens and of Anonymous. The actions of this regime will not be forgotten, nor will they be forgiven.

When people are faced with such injustices, Anonymous hears those cries, and we will assist in bringing to justice those who commit criminal acts against the innocent. We will not remain silent and let these crimes against humanity continue. The attempts to censor the Bahrainian people from the Internet - which prevents them from communicating their struggle to the outside world - are despicable stratagies and shows the cowardness of this regime, as well as the measures they are willing to take to cover their crimes.

To the people of Bahrain: We stand with you against your oppressors. This is not only your struggle, but one of people who are struggling for freedom all over the world. With the recent success in Tunisia and Egypt, we believe your revolution will succeed. Your brave actions will maintain the momentum of revolution for citizens all around the world wishing to regain their own freedoms.

We are Anonymous.
We are legion.
We do not forgive.
We do not forget.
Expect us.

A manifesto of a hacktivist campaign. Anonymous published this manifesto before it launched “OpBahrain” attacks against the Bahrainian government. The manifesto describes clear motivation for the attacks.

Rights and permissions

Reprints and permissions

Copyright information

About this paper

Cite this paper

Nurmi, J., Niemelä, M.S. (2018). PESTEL Analysis of Hacktivism Campaign Motivations. In: Gruschka, N. (eds) Secure IT Systems. NordSec 2018. Lecture Notes in Computer Science(), vol 11252. Springer, Cham. https://doi.org/10.1007/978-3-030-03638-6_20

.RIS↓ .ENW↓ .BIB↓

DOI	Published	Publisher Name
https://doi.org/10.1007/978-3-030-03638-6_20	02 November 2018	Springer, Cham

Print ISBN	Online ISBN	eBook Packages
978-3-030-03637-9	978-3-030-03638-6	Computer Science Computer Science (R0)

Publish with us

Policies and ethics

Search

Search by keyword or author