Vulnerability at Home: Domestic Factors of Cyberterrorism in SCO Countries

Jingbo Liao(✉)

Sichuan University, Chengdu, China
1976562130@qq.com

Abstract. As the latest hybridization of cyberspace and terrorism in the twenty-first century, cyberterrorism transcends national boundaries and poses an unprecedented non-traditional threat to any entities accessible to the Internet, including governments, corporates and civilians. The Shanghai Cooperation Organization is among the first international organizations which have combined anti-terrorist cooperation with Internet governance. However, few attempts have been made to analyze the cause of cyberterrorism in SCO members systematically and quantitatively. This study built up a connection between domestic situations and the occurrence of cyberterrorism by computational method which included factor analysis, OLS regression and spatial regression. Results suggested that three significant factors underlying cyberterrorism in SCO countries are Internet Factor, Dimensional Factor and Social Factor. In addition, the comparison of their relative influence is: Internet Factor the most significant, Social Factor slightly less powerful and Dimensional Factor much less remarkable than the former two. Theoretical and practical contributions are also discussed in this paper.

Keywords: cyberterrorism · SCO · Internet governance · factor analysis · regression analysis

1 Introduction

Imagine that you are browsing websites while being tracked and attacked by a terrorist over hundreds of miles away from you and more incredibly, the weapon causing damage to you is simply the Internet instead of guns or bombs. Terrorism has been in the limelight of global governance and international cooperation since the September 11 Attacks (Miller 2019). With the rapid development of information technology during the past two decades, cyberterrorism, a new variant of terrorism, has been increasingly possible to impose a non-traditional threat to any natural individuals or political entities. To counterbalance cyberterrorism, inter-governmental organizations (regional or global) which involve more than one country are expected to take actions, considering its superb capability to transcend national borders. Among them the Shanghai Cooperation Organization is ought to be granted with top priority.

Seldom has there been a technology or a product which could spread across the world more abruptly and immediately than the expansion of cyberterrorism. Internet is

N. Akhtar et al. (Eds.): PMIS 2023, AHIS 8, pp. 679–690, 2023.
https://doi.org/10.2991/978-94-6463-200-2_70

undoubtedly the most advanced information carrier among modern media and terrorism is perhaps the most preeminent origin of violent crime (Jarvis and Macdonald 2014). The hybridization of the two has caused tsunami-like impact on the world. With the competence to break the confines of both time and space, cyberterrorists not only use the Internet as a weapon to impose threats to political, economic or technological targets but also disseminate extreme ideas such as Nazism and fundamentalism by the Internet. More specifically, the traditional boundary between "cyberattack", "cybercrime", "cyberespionage" and "network warfare" which once dominates various debates about science, law and politics has already blurred to the extent that cyberterrorism which involves all of them is now worth the most elaborate research and resistance.

Founded on the basis of the Shanghai Convention against Terrorism, Separatism and Extremism (2001) which was jointly signed by the People's Republic of China, Russian Federation, the Republic of Kazakhstan, the Republic of Tajikistan, the Republic of Uzbekistan and Kyrgyz Republic, the Shanghai Cooperation Organization (SCO) is one of the earliest inter-governmental international organizations who took the initiative to pay attention to the topic of terrorism and establish a relatively developed a counter-cyberterrorism institution. The significance of SCO derives from not only its efforts to fight cyberterrorism but also the geographical location of its member states (Blank 2013). Stretching from the Pacific Ocean in the east to the Black Sea in the west and covering from the Baikal Lake in the north to the Persian Gulf in the south, SCO countries dominate a vast land on the Eurasian Continent, smaller than the "World-Island" but larger than the "Heartland" according to the geopolitical theory of Halford John Mackinder. Diversity of ethnic groups and fragmentation of religions had laid a solid foundation for the takeover of political vacuum by separatism, fundamentalism and extremism after the Collapse of Soviet Union in 1991. At the dawn of the 21st century, a majority of SCO countries were identified as emerging markets with their Internet users and industries expanding swiftly. Here comes the worst-case scenario that terrorist organizations and individuals have taken advantage of the information revolution and transformed the traditional terrorism into cyberterrorism (Yunos et al. 2017). Now SCO countries find themselves incapable of action faced with the common but differentiated threat from cyberterrorism since it is transnational, asymmetrical and beyond visual range. Before we are able to retaliate effectively, it is of great importance to have an insight into a question: why does cyberterrorism happen in SCO countries and what are the specific factors within their territories promoting it? Maybe ethnic and religious situations mentioned above could make some sense. However, there is limited research which has addressed domestic causes for the incidence of cyberterrorism systematically and quantitatively.

Here this research tries to fill this research gap by exploring in what way and to what extent specific domestic factors influence cyberterrorism in SCO countries. Particularly, this research transformed primitive variables extracted from extant literature into comprehensive factors and analyze their respective influence on cyberterrorism in SCO countries. This study thus contributes to the extant literature on the source of cyberterrorism by emphasizing quantitative research from a domestic view.

1.1 The Concept of Cyberterrorism

There have been amounts of research and debate about the concept of cyberterrorism since the end of twentieth century without a universal conclusion. The origin or constitution of cyberterrorism attracts most attention of research at the beginning and here comes the "convergence hypothesis". It has been considered to be the convergence of cyberspace which belongs to the virtual world, and terrorism which belongs to the physical world (Watt and Janczewski 2009).

Then academia concentrates more on the function of cyberterrorism and here comes the "attack hypothesis", probably influenced by the behaviorism school. The whole attack process could be interpreted into three key questions: who attack, what to to attack and what to achieve by the attack. The attackers are considered to be terrorists from sub-national groups and clandestine agents (Conway 2002). They are supposed to attack or threat to attack the Internet, data stored in it and some relevant infrastructure in order to intimidate the government or civilians into compromising on some political or social problems (Straub 2020).

1.2 Factors Behind Cyberterrorism

Extant research also focuses on factors that underlie the formation and development of cyberterrorism and these factors can be roughly sorted into three categories respectively about Internet, society and dimension. The information revolution, for instance, has exacerbated the asymmetry of power between international relations and cyberspace, turning network-developed countries more and more vulnerable to cyberterrorism (Nye 2010).

For a certain country or area, the scale effect is widely referred to as a multiplier to the threat posed by cyberterrorism. The economic loss brought about by cyberterrorism is contingent on the scale of gross domestic product (GDP) and the relevant percentage of Internet economy in it. In terms of political risk, both typical terrorism and cyberterrorism spread widely in the post-Soviet space, especially Central Asia where the collapse of the USSR produced enormous political vacuum, making the vast and densely-populated Eurasia heartland the hotbed of terrorists (Horsman 2005).

Society is perhaps the most common alternative to the state-oriented analysis because it transcends national boundaries. Traditional society disintegrates into fragmented units and releases atomistic individuals as a result of globalization, potentially strengthening the mobilizing capacity of cyberterrorism (Jarvis et al. 2015). The effect of cyberterrorism also varies in different social strata, especially in societies with rigid hierarchy and severe polarization, because the sense of loss and other negative emotions of the underclass could be easily tapped by extremist organizations closely connected with cyberterrorism (Tinnes 2021).

1.3 Anti-cyberterrorist Cooperation in SCO

In terms of international joint actions against cyberterrorism, few institutions could be more experienced and established than the multi-lateral cooperation of the Shanghai Cooperation Organization which is among the first inter-governmental organizations to set out for containing cyberterrorism (Nye and Sharma 2015). The main goal is to fight terrorism, extremism and separatism online without intervening in domestic affairs of member states. In regard to the relationship between SCO and other international actors, anti-cyberterrorist cooperation shares the issue linkage with U.S.'s power projection in Central Asia, China's Belt and Road Initiative and Afghanistan's geopolitics (Lanteigne 2006).

H1. SCO countries tend to have a higher risk of cyberterrorism with a more developed Internet industry.
H2. SCO countries tend to have a higher risk of cyberterrorism with larger population, territory or economy.
H3. SCO countries tend to have a higher risk of cyberterrorism with a more disordered society.
H4. Geographical proximity is either a mediator or a competing explanation for the effect of domestic factors on the risk of cyberterrorism through the transboundary spillover effect of domestic situations or cyberterrorist events.

2 Data Description and Method

Mainly focusing on cyberterrorism in SCO countries, this study was aimed at its nine members in total, China, Russia, Kazakhstan, Kyrgyz, Uzbekistan, Tajikistan, India, Pakistan and Iran. To figure out factors behind cyberterrorism, traditional method is doomed with intrinsic paradox. The potential factors evaluated and picked by researchers are heavily influenced by their subjectivity to an extent that the independence of factors is not firmly guaranteed and the relationship between them is not explicitly analyzed because of latent correlation and information overlap. To overcome this dilemma, this research was conducted in three steps.

Firstly, through text analysis, this research extracted potential factors which were frequently discussed and recommended in the extant literature, and embodied them with ten primitive variables which were Internet Users (V1), Territory (V2), Internet Penetration (V3), Population (V4), Fixed Broadband Penetration (V5), ICT Development Index (V6), Mobile Broadband Penetration (V7), Gini Coefficient (V8), Social Stability Index (V9), Gross Domestic Product (V10).

Secondly, through factor analysis, this research transformed primitive variables which may be sophisticatedly correlated with one another into several comprehensive factors which were able to classify, include and represent previous variables by probing into the inner structure of the correlation matrix of them.

Thirdly, through regression analysis, this research evaluated the influence of domestic factors on cyberterrorism with comprehensive factors as independent variables and the frequency of cyberterrorist events as the dependent variable.

The list of databases used in this study is as follows, World Bank (WB), International Telecommunication Union (ITU), Institute for Economics and Peace (IEP), Centre for Strategic and International Studies (CSIS), Global Terrorism Database (GTD). All data involved in factor analysis and regression analysis is the average within two decades from 2000 to 2020 in consideration of durability and validity.

3 Result

Before the main analysis, this research conducted a KMO and Bartlett's test to check if this research is appropriate for a factor analysis. The result rejected the hypothesis that the correlation coefficient matrix is a unitary array (KMO = 0.667, Sig < 0.05), suggesting that the correlation between variables is suitable for a factor analysis. Checking the communality, it was assured that the information would be effectively extracted by factors later and the prospect of a factor analysis would be successful.

As for the main analysis, this research first extracted factors through principal component analysis and detailed information is shown in Table 1 and Fig. 1. It can be concluded that the factors were able to fully represent and equivalently substitute the primitive variables (IE1 + IE2 + IE3 = 89.676%, IE3 $>$ 1, IE4 $<$ 1). And the first three factors exceled more prominently than the following ones in terms of explanatory power. Therefore, Component 1, Component 2 and Component 3 were chosen to be the three common factors.

Then, this research rotated factors through Promax with Kaiser normalization and detailed information is shown in Table 2 and Table 3. From the comparison between the unrotated component matrix and the rotated component matrix, primitive variables could be distributed to different common factors: (1) V3, V5, V6, V7 held higher factor loading in Component 1 (V3 = 0.915, V5 = 0.902, V6 = 0.949, V7 = 0.608) so that we defined it as the Internet Factor (F1); (2) V1, V2, V4, V10 held higher factor loading in Component 2 (V1 = 0.967, V2 = 0.816, V4 = 0.954, V10 = 0.866) so that we defined it as the Dimensional Factor (F2); (3) V8, V9 held higher factor loading in Component 3 (V8 = 0.917, V9 = 0.778) so that we defined it as the Social Factor (F3). After it, we figured out the factors' score by using the component score coefficient matrix (see table 4).

Extraction Method: Principal Component Analysis.

Extraction Method: Principal Component Analysis.

Rotation Method: Promax with Kaiser Normalization.

Table 1. Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	total	% of Variance	Cumulative%	total	% of Variance	Cumulative%	total	% of Variance	Cumulative%
1	4.962	49.624	49.624	4.962	49.624	49.624	4.356	43.561	43.561
2	2.974	29.738	79.363	2.974	29.738	79.363	3.043	30.428	73.989
3	1.031	10.313	89.676	1.031	10.313	89.676	1.569	15.687	89.676
4	0.494	4.938	94.614						
5	0.247	2.467	97.081						
6	0.169	1.685	98.767						
7	0.094	0.945	99.711						
8	0.029	0.289	100.000						
9	0.000	0.000	100.000						
10	0.000	0.000	100.000						

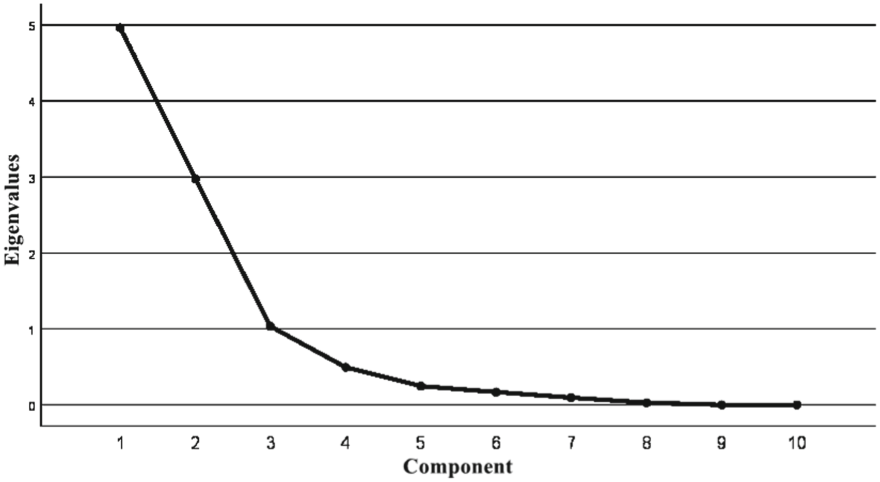

Fig. 1. Scree Plot of Eigenvalues

Table 2. Unrotated Component Matrix

	Component		
	1	2	3
V1	0.675	0.664	-0.310
V2	0.834	-0.165	0.265
V3	0.732	-0.601	-0.187
V4	0.516	0.720	-0.368
V5	0.985	-0.179	0.019
V6	0.832	-0.483	-0.068
V7	0.185	-0.881	-0.165
V_8	0.342	0.540	0.698
V_9	0.801	-0.126	0.370
V_{10}	0.780	0.525	-0.195

Next, this research regressed the incidence of cyberterrorism (C) on Internet, Dimensional and Social Factors (F1, F2 and F3) through the OLS model, and detailed information is shown in Table 5, Table 6 and Table 7. It can be concluded that the model was robust (Adjusted R2 = 0.925, F = 33.867, SigF < 0.05). The results showed that all three common factors had a positive and significant effect on the incidence of cyberterrorism (B1 = 12.915, p1 < 0.05, B2 = 4.587, p2 < 0.05, B3 = 11.050, p3 < 0.05). The model equation of domestic factors behind cyberterrorism was C = 12.915 F1 + 4.587 F2 + 11.050 F3 + 35.222. The relative significance of three factors followed as Internet Factor > Social Factor > Dimensional Factor.

Table 3. Rotated Component Matrix

	Component		
	1	2	3
V_1	0.181	0.967	0.157
V_2	0.308	0.816	0.181
V_3	0.915	0.036	-0.304
V_4	0.012	0.954	0.103
V_5	0.902	0.353	0.110
V_6	0.949	0.114	-0.128
V_7	0.608	-0.454	-0.512
V_8	0.072	0.224	0.917
V_9	0.411	0.141	0.778
V_{10}	0.355	0.866	0.213

Table 4. SCO Countries' Factor Score

	F_1	F_2	F_3
Kazakhstan	0.862	-0.432	-1.216
Kyrgyz	-0.234	-0.404	-1.295
Tajikistan	-0.821	-0.337	0.088
Iran	-0.716	-0.775	1.941
Uzbekistan	0.114	-0.466	-0.376
China	0.911	2.139	0.529
Russia	1.815	-0.826	0.749
India	-0.877	1.205	-0.188
Pakistan	-1.053	-0.103	-0.231

Table 5. Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.976a	0.953	0.925	4.940

Finally, this research examined the effect of geographical proximity by the method of spatial econometrics which was based on the comparison of the Queen continuity spatial weighted matrix and the K-Nearest Neighbor spatial weighted matrix (KNN). Detailed information is shown in Fig. 2. And Table 8. It can be concluded that the

Table 6. ANOVAa

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2479.533	3	826.511	33.867	0.001b
	Residual	122.023	5	24.405		
	Total	2601.556	8			

Table 7. Coefficientsa

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	35.222	1.647		21.390	0.000
	F1	12.915	1.747	0.716	7.395	0.001
	F2	4.587	1.747	0.254	2.626	0.047
	F3	11.050	1.747	0.613	6.326	0.001

spatial autocorrelation was far from significant enough to carry our examination into deeper research because SCO countries were evenly located in four quadrants, and the p-values of Moran's I for both Queen and KNN were overly high (0.485 and 0.129 respectively). Besides, the results of LM test and formal spatial regression further rejected the assumption that either Spatial Lag Model or Spatial Errors Model could be used to explain the data since neither proved to be significant.

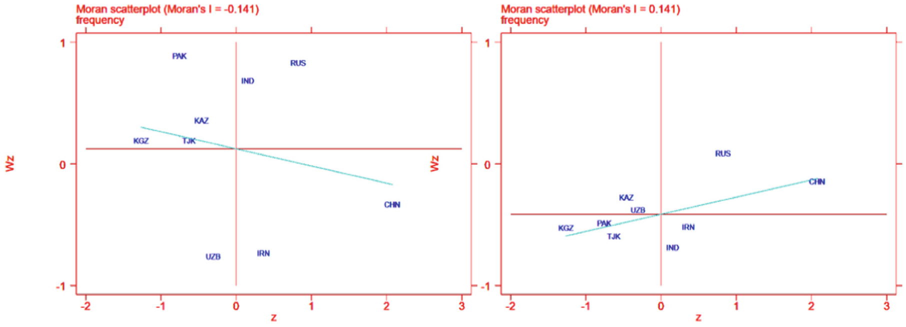

Fig. 2. Moran Scatterplots of Queen and KNN Spatial Weighted Matrices

Table 8. LM Test and Lag-Error Model

	Queen (p-value)	KNN (p-value)
lag LM	0.104	0.150
lag Robust LM	0.127	0.059
error Moran's I	1.061	0.284
error LM	0.327	0.486
error Robust LM	0.425	0.670
rho	0.190	0.113
lambda	0.770	0.055
global spatial autocorrelation	0.485	0.129

4 Discussion

This study examined the effect of domestic situation on the occurrence of cyberterrorism in SCO countries. This research found that plenty of potential variables proposed by preceding researchers could be summarized and classified into three comprehensive factors which exert respective influence on domestic cyberterrorism in varying degrees.

The current study makes several theoretical contributions. First of all, previous research on the causes of cyberterrorism has mainly focused on ambiguous suggestion and critical analysis, lacking in meticulous classification and comparative assessment. By means of empirical study and quantitative method, this research implies that it is flexible to accurately evaluate the respective influence of potential factors. In addition, previous research about international organization's performance on non-traditional security like SCO on cyberterrorism has chiefly concentrated on transnational cooperation such as intelligence sharing and joint action, and supranational entities such as EU and UN themselves (Price 2012). Based on domestic view, this work reveals a promising approach to explore the origin of cyberterrorism in SCO countries at a more microscopic level.

The current study also has several practical implications. With elaborate research into domestic factors behind cyberterrorism, we can provide pragmatic advice for countries caught fighting it. To begin with, since it is impracticable to make fundamental change with national dimension such as population and territory, policy makers are expected to pay attention to Internet development and social institution. In terms of Internet, government should lay down an up-to-date set of regulations and laws to keep IT technologies and industries under the supervision of national security and moral ethics instead of simply restricting their development (Baezner 2020). With regard to society, it is of great significance to set up a fair and comprehensive distribution system to prevent the emergence of cyberterrorists because of salary polarization and class contradiction.

There are some limitations worth noting, which require further investigation. In the first place, this research focused only on domestic affairs and potentially ignored external aspects. There are many international factors such as population shift, foreign direct investment and of course Internet for its transnational character (Westby 2007). For example, illegal immigration may play an intensive role in the formation of cyberterrorism because of its ambiguous relation with terrorist penetration, which is contingent on geographical proximity (Choi 2018). Besides, this study mainly discussed the cyberterrorism within SCO. It remained unclear that to what extent the principle here could be applied to other countries across the globe. Thus, it might be interesting to conduct new research in a broader international horizon.

5 Conclusions

In the dawn of the 21st century, cyberterrorism as a variant of terrorism has become a new source of non-traditional security threat. Considering the free, open and interdependent nature of the Internet, terrorists effortlessly transcend real political borders and launch swift, accurate and destructive attacks on any entities accessible to the Internet, creating a tsunami-like impact on the international community and negative spillover effect on physical world. The Shanghai Cooperation Organization is the first regional inter-governmental organization which has tried to unite its members and counterbalance cyberterrorism. However, previous studies paid little attention to domestic affairs as the content and quantitative analysis as the method to analyze factors underlying cyberterrorism in SCO countries. In order to fill this research gap, this study built up a connection between domestic situations and cyberterrorism in SCO countries through the combination of factor analysis and regression analysis. The results showed the following: (1) Three significant factors behind cyberterrorism in SCO countries are Internet Factor, Dimensional Factor and Social Factor; (2) When a country holds immense Internet penetration and prosperous ICT industries, the risk of cyberterrorism is higher than a country which does not; (3) When a country has huge population, vast territory and considerable GDP, the risk of cyberterrorism is higher than a country which does not; (4) When a country get stuck in income polarization and social turmoil, the risk of cyberterrorism is higher than a country which does not; (5) Geographical proximity is not significant enough to play a role in the risk of cyberterrorism; (6) The rank of relative influence is: Internet Factor the most significant, Social Factor slightly less significant and Dimensional Factor much less remarkable than the former two.

References

1. Baezner, M. (2020). Cybersecurity in switzerland: Challenges and the way forward for the swiss armed forces. Connections, 19(1), 63–72. https://doi.org/10.11610/Connections.19.1.06

2. Blank, S. (2013). Making Sense of the Shanghai. Georgetown Journal of International Affairs, 14(2), 39–49. https://www.jstor.org/stable/43134410
3. Choi, S. W. (2018). Does restrictive immigration policy reduce terrorism in western democracies? Perspectives on Terrorism, 12(4), 14–25. https://www.jstor.org/stable/26482976
4. Conway, M. (2002). What Is Cyberterrorism? Current History, 101(659), 436–442. https://doi.org/https://doi.org/10.1525/curh.2002.101.659.436
5. Horsman, S. (2005). Themes in official discourses on terrorism in Central Asia. Third World Quarterly, 26(1), 199–213. https://doi.org/https://doi.org/10.1080/0143659042000322982
6. Jarvis, L., & Macdonald, S. (2014). Locating Cyberterrorism: How Terrorism Researchers Use and View the Cyber Lexicon. Perspectives on Terrorism, 8(2), 52–65. https://www.jstor.org/stable/26297136
7. Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage. Perspectives on Terrorism, 9(1), 60–75. https://www.jstor.org/stable/26297327
8. Lanteigne, M. (2006). In medias res: The development of the Shanghai Co-operation Organization as a security community. Pacific Affairs, 79(4), 605–622. https://doi.org/https://doi.org/10.5509/2006794605
9. Miller, G. D. (2019). Blurred lines: The new "domestic" terrorism. Perspectives on Terrorism, 13(3), 66–78. https://www.jstor.org/stable/26681909
10. Nye, J. S. (2010). The future of American power dominance and decline in perspective. Foreign Affairs, 89(6), 2–12. https://www.jstor.org/stable/20788711
11. Nye, J. S., & Sharma, T. (2015). Is the American century over? Political Science Quarterly, 130(3), 393–400. https://doi.org/https://doi.org/10.1215/10474552-3488093
12. Price, E. (2012). Literature on Terrorism, Media, Propaganda & Cyber-Terrorism. Perspectives on Terrorism, 6(1), 92–103. https://www.jstor.org/stable/26298558
13. Straub, V. J. (2020). Beyond kinetic harm and towards a dynamic conceptualization of cyberterrorism. Journal of Information Warfare, 20(Guterres 2020), 1–27. https://www.jstor.org/stable/https://doi.org/10.2307/27124996
14. Tinnes, J. (2021). Bibliography: Terrorism and the Media (including the Internet). In Perspectives on Terrorism (Vol. 15, Issue 2). https://www.jstor.org/stable/26626869
15. Watt, A., & Janczewski, L. (2009). Cyber Terrorism Awareness Within New Zealand Critical Infrastructure. Journal of Information Warfare, 8(3), 27–38. https://www.jstor.org/stable/https://doi.org/10.2307/26486765
16. Westby, J. R. (2007). Countering Terrorism With Cyber Security. Jurimetrics, 47(3), 279–294. https://doi.org/https://doi.org/10.1142/9789812709233_0036
17. Yunos, Z., Mohd, N., Ariffin, A., & Ahmad, R. (2017). Understanding cyber terrorism from motivational perspectives: A qualitative data analysis. European Conference on Information Warfare and Security, ECCWS, 16(4), 550–557. https://www.jstor.org/stable/https://doi.org/10.2307/26504114