Received:
April 13, 2022

Revised:
December 13, 2022 &
December 21, 2022

Published:
December 27, 2022

Journal of Politics and International Studies
Vol. 8, No. 2, July–December 2022, pp.45–57

From Cyber Security to Cyber-terrorism: A New Emerging threat for Europe and the challenges for EU

Ahmed Ali Naqvi
Lecturer,
Department of Political Science
University of the Punjab, Lahore, Pakistan
Correspondence: ahmad.polsc@pu.edu.pk

Amyda Javaid
M.Phil. in International Relations,
Department of Political Science
University of the Punjab, Lahore, Pakistan

Dr. Iqra Jalal
Ph.D. in Political Science,
Department of Political Science
University of the Punjab, Lahore, Pakistan

ABSTRACT

Cyber technology is widely used to share information with audience around the world, as it is relatively cheaper and easy to access. Cyber Security issues range from hacking to Cyber Terrorism. The threat of terrorism within the cyber space is increasing as today humans' interaction with cyber technology is more than ever in human history. Similarly, the terrorist organisations have moved towards technological orientation to fulfil their agendas not only by causing physical damage but also by destructing and manipulating sensitive data that may harm the economy and security of a state. Cyber technology is used by terrorists to communicate, propagate, radicalize, recruit or influence the people mainly because it is multifunctional and can be used as a modern tool for warfare. The intention and motivation of the individuals or groups behind these acts differentiate between hacktivism, cyber-attacks and cyber-terrorism. The potential threats of cyber terrorism to European Union for example within the industrial sector the possible threat from cyber terrorists in Industrial Control System (ICS) and the failure of these technologically advanced states to provide reliable security system, pose a threat to their socio-political, economic and military sectors. This paper discusses the aims and objectives of terrorists behind these attacks. How far have they been successful in causing a serious harm to the security of these states? What strategies by far have been adopted by European Union to counter this threat? To what extent these strategies have been effective in offsetting the threat of cyber terrorism? The loopholes in cyber security system allow the terrorists to reach the confidential data of public and private organisations. So, efficient measures and strict action against the criminals in general and terrorists in particular along with the cooperation between government organisations and private software companies can strengthen the networks against cyber-terrorism.

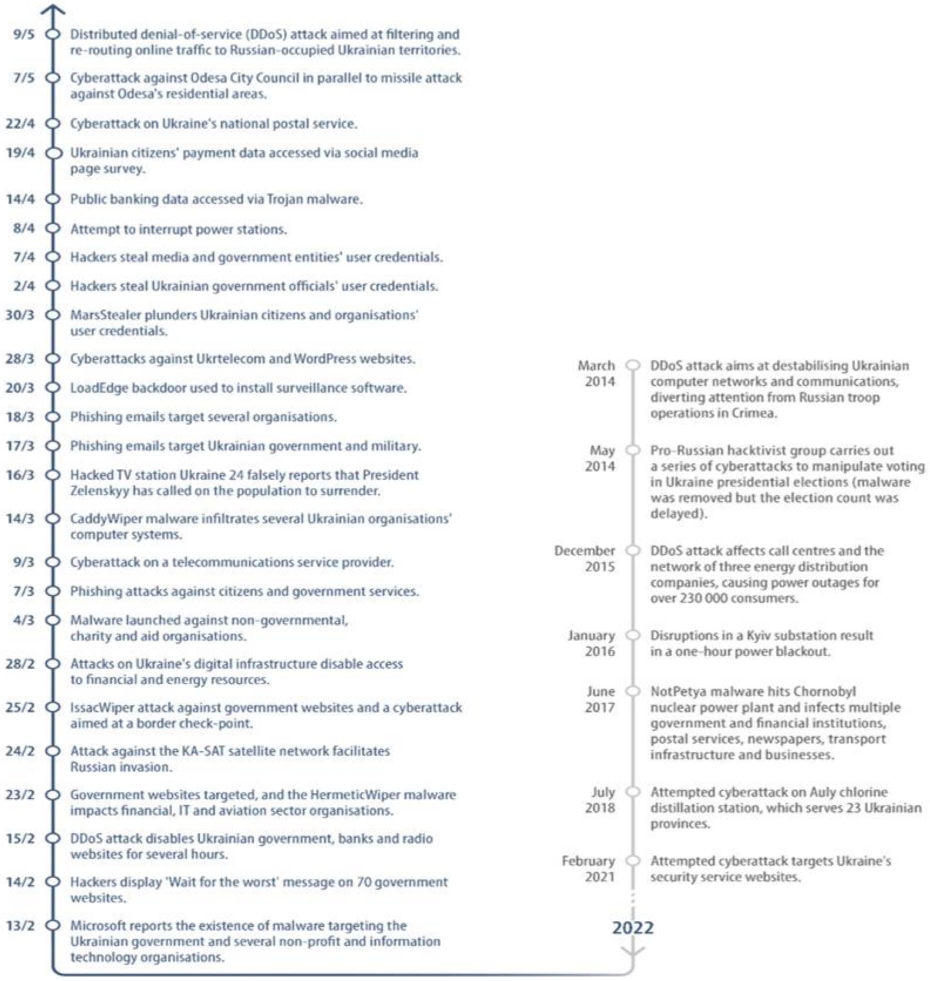
Keywords: *Terrorism, Cyber-terrorism, Cyber warfare, European Union, Cyber security*

Introduction

Terrorism is usually explained as the use or threat of violence to fulfil a political cause. The complexity and ambiguity in defining terrorism is the reason that we have not achieved a universal consensus on a single definition of terrorism (Max Roser, 2013). Although the term has no universally agreed definition but still terrorism can be understood as a method in which violence or threat of violence is used to gain ideological or political goals by spreading fear. The emergence of cyberspace and Information and Communications Technology has ushered in the digital age. The digital age has resulted in positive as well as negative consequences for all actors inside and outside the cyber domain. It has empowered individuals around the world and helped revolutions on its way as was seen with the Arab Spring. It has driven economic growth and created new markets. However, increase in cyber-crime and major cyber-attacks in Estonia 2007, Georgia 2008 and Iran 2010 along with cases of cyber espionage revealed in 2013, has all shown that serious risks and threats are evolving with cyberspace. Due to the rise of cyber incidents along with increased concern over critical infrastructure reliability of cyberspace, many nation-states are considering cyberspace the greatest security challenges of this century. (Nielsen, 2016) There are various other examples that how the organisations of a state that are backed by their governments have been successful in using hacking techniques to harm their enemy states by disrupting their financial, political or security systems, but still we see many security experts are hesitant in calling cyberterrorism a real threat which has an ability of causing serious long-term damage and the reason they give is that a terror attack often leads to loss or at least harm to life but a computer attack has never achieved this or caused any massive destruction because to them a homemade bomb will always be much more effective than a computer or electronic attack which does not involve physical damage or bloodshed. (Cyberterrorism: Myth or reality?, 2007) Fundamentally, the EU perceives that the insecurities or threats associated with cyber space are merely technical faults which can be handled. However, United States of America in 2009 marked cyber-security as its highest priority in national security. "The EU Cybersecurity Strategy highlights five strategic priorities that shall combat the issues emerging from cyberspace. (1) Achieving cyber resilience, (2) Drastically reducing cybercrime, (3) Developing defence policy and capabilities related to the Common Security and Defence Policy (CSDP), (4) Develop the industrial and technological resources for cybersecurity and (5) Establish a coherent international cyberspace policy for the European Union and promote EU values". (Nielsen, 2016)

In 2004 EU formed a very advanced cyber security institution ENISA, the European Union Agency for Network and Information Security which is responsible for detecting threats and vulnerabilities to EU within the cyberspace. This paper focuses on the emerging threats of cyber-terrorism that EU is facing and the policies and plans it is making to overcome this contemporary issue.

Most recently, Ukraine War has not only exposed but also intensified the threats of Cyber-attacks by elements linked with states. Ukraine is not the first target of Cyber War but certainly the most important case of significant use of cyber warfare by rival states. Europe has not seen such massive cyber-attacks on its cyber space ever before. This cyber war on one hand provided major challenges to European Cyber security and on the other hand provided opportunity to strengthen its guards against more sophisticated future cyber-attacks. (Cyber War and Ukraine, 2022) It also tests their existing policies, tools, knowledge, expertise and in broader sense their resilience to such warfare. Here is the timeline of Cyber-attacks since Ukraine War began in February 2022.



9/5 Distributed denial-of-service (DDoS) attack aimed at filtering and re-routing online traffic to Russian-occupied Ukrainian territories.

7/5 Cyberattack against Odesa City Council in parallel to missile attack against Odesa's residential areas.

22/4 Cyberattack on Ukraine's national postal service.

19/4 Ukrainian citizens' payment data accessed via social media page survey.

14/4 Public banking data accessed via Trojan malware.

8/4 Attempt to interrupt power stations.

7/4 Hackers steal media and government entities' user credentials.

2/4 Hackers steal Ukrainian government officials' user credentials.

30/3 MarsStealer plunders Ukrainian citizens and organisations' user credentials.

28/3 Cyberattacks against Ukrtelecom and WordPress websites.

20/3 LoadEdge backdoor used to install surveillance software.

18/3 Phishing emails target several organisations.

17/3 Phishing emails target Ukrainian government and military.

16/3 Hacked TV station Ukraine 24 falsely reports that President Zelenskyy has called on the population to surrender.

14/3 CaddyWiper malware infiltrates several Ukrainian organisations' computer systems.

9/3 Cyberattack on a telecommunications service provider.

7/3 Phishing attacks against citizens and government services.

4/3 Malware launched against non-governmental, charity and aid organisations.

28/2 Attacks on Ukraine's digital infrastructure disable access to financial and energy resources.

25/2 IssacWiper attack against government websites and a cyberattack aimed at a border check-point.

24/2 Attack against the KA-SAT satellite network facilitates Russian invasion.

23/2 Government websites targeted, and the HermeticWiper malware impacts financial, IT and aviation sector organisations.

15/2 DDoS attack disables Ukrainian government, banks and radio websites for several hours.

14/2 Hackers display 'Wait for the worst' message on 70 government websites.

13/2 Microsoft reports the existence of malware targeting the Ukrainian government and several non-profit and information technology organisations.

March 2014 DDoS attack aims at destabilising Ukrainian computer networks and communications, diverting attention from Russian troop operations in Crimea.

May 2014 Pro-Russian hacktivist group carries out a series of cyberattacks to manipulate voting in Ukraine presidential elections (malware was removed but the election count was delayed).

December 2015 DDoS attack affects call centres and the network of three energy distribution companies, causing power outages for over 230 000 consumers.

January 2016 Disruptions in a Kyiv substation result in a one-hour power blackout.

June 2017 NotPetya malware hits Chornobyl nuclear power plant and infects multiple government and financial institutions, postal services, newspapers, transport infrastructure and businesses.

July 2018 Attempted cyberattack on Auly chlorine distillation station, which serves 23 Ukrainian provinces.

February 2021 Attempted cyberattack targets Ukraine's security service websites.

Source: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Literature Review

The definitional dilemma of terrorism is well known. The difficulty in defining terrorism is because every state has its own definition of terrorism. An individual may be a terrorist for one state, but he'll be a freedom fighter for another state. Moreover, the difficulty in differentiating between acts like state sponsored terrorism, guerrilla warfare, separatism or fight for national independence and the ambiguity in terms like state sponsored terrorism and non-combatants make it difficult to reach a universally accepted definition of terrorism. (Wojciechowski, 2009; Libaw, 2016; Schmid, 2011)

Generally, terrorism can be defined as an act of violence directed against the civilians by actors who may cause serious physical harm or even death of the individuals to fulfil their political interests by pressurizing an international organization or government to disrupt the functioning of a state. (UN General Assembly Resolution, 1994; UN Security Council Resolution, 2004; European Union, 2002; US Patriotic Act, 2001).

With the advent of internet and rise of technology individuals and clandestine agents are moving from traditional methods of terrorism to advanced methods. The merge of terrorism and cyber space is called cyber-terrorism. It uses the illegal attacks and threats of attacks against computers or networks and the hacking or manipulation of sensitive or confidential data to harm the security of a state. (Yunos, 2017; Metropoulos and Platt, 2018). Cyber technology is used by terrorists to communicate, propagate, to train or plan and radicalize, recruit or influence the people as it is multifunctional and can be used as a modern tool for warfare. The intention and motivation of the individuals or groups behind these acts differentiate between hacktivism, cyber-attacks and cyber-terrorism. (Saqib khan and Khalid Manzoor butt, 2017; Zerzri, 2017)

Pure cyber terrorism can be differentiated into following three categories. The support to the operations of terrorist groups through online activities which is known as enabling, the interference in the information technology of opponents through online means which is known as disruption and the cyber-attacks to cause injury or physical damage by imitating digital control systems and operation technology which is known as destruction (Evan, 2017; Zerzri, 2017).

The potential threats of cyber-terrorism in the industrial sector include the possible threat from Cyber terrorists in the Industrial Control System (ICS). STUXNET Malware is an example of how vulnerable ICS systems potentially are. Industrial control systems not even connected to internet are also exposed to this threat. (Pretoriou, 2016; ANSSI, 2014; Holloway, 2015) Cyber terrorism however portrayed as a major threat to Europe and America but there are a few scholars who consider it not a major threat but a myth that is obvious because of the great reliance of human societies on internet but till now there has not been any large scale case of cyber terrorism recorded, that resulted in mass killings like the conventional method of terrorism. (Lachow, 2011; Collingburn, 2016; Gorge, 2007)

In 2007 cyber-attacks on the websites of Estonian parliament, government ministries, banks and newspapers were a wakeup call for the government. Than in 2014 three attacks to hack the Ukrainian Presidential elections showed that how cyber space can be exploited by various agents to harm the states and fulfil their agendas. Thus, EU member states have cooperated through capacity building measures to overcome this threat and EU has recently introduced its EU Cyber Security Strategy. (Clayton, 2014; Schulze, 2018; Sliwinski, 2014)

The European counter terrorism centre (ECTC) was launched in January 2016 to counter this threat, followed by a decision on 20th November 2015 from the Justice and Home Affairs Council. Through this platform the member states can share information and increase their operational cooperation about the examining and investigation of foreign terrorist fighters and the unlawful trade of fire arms and terrorist financing.

Methodology

For the purpose of data collection, this study involves qualitative technique of content analysis. With the increasing use of Internet and rising insecurities in cyber-space a new threat of cyber-terrorism is emerging that is threatening the security of the states. As cyber-space has become an important tool for terrorists to fulfil their agendas, new policies are being made by states to overcome this threat by securing their cyber-space. So, by using the descriptive method of analysis we will analyse the existing data available for this study. Also, we will observe the trends and techniques being used by European states specifically EU to counter this threat through observational technique which will help to analyse the viewpoints of various scholars and their take regarding this emerging threat and for that a mixed method approach has been used. Also, the major and minor events of cyber-terrorism will help to differently conclude my study in a remarkable way.

For research material I have consulted various qualitative data and few of the quantitative data to strengthen my qualitative research. My sources for research include books, journal and periodical articles, reports, research papers and website links.

Theoretical Framework

The major issue in defining terrorism is the theoretical explanation of the phenomenon of terrorism and the intentions of terrorists behind this act, which is also a reason behind the definitional dilemma of terrorism. The major theories which explain the phenomenon of terrorism and cyber-terrorism are Realism either classical or neo-realism, constructivism, rational choice theory, structural theory, domestic determinants theory, cognitive and psychological approaches. These theories focus on various points of terrorism and cyber-terrorism and are helpful in answering the questions why the terrorists engage in violent activities? What are the reasons behind the use of cyber-space by terrorists? How can European Union states collaborate to counter the threat of cyber-terrorism?

The realist theory best explains the phenomenon of terrorism and explains the reason that why terrorists indulge in such extremist activities, what political and economic or social gains they have from this act along with the rational choice theory that tries to explain the intentions and causes behind such acts. However, the constructivist theory in the contemporary world best explains the phenomena of terrorism and cyber-terrorism because the basic nature of terrorism is a ‘social construct’, it offers itself to constructivist approach. As it is the international system and its rules and norms which tend to construct and reconstruct identities further shaping the material and non-material interests of the states and the individuals. In the process of analysing constructivism’s place among notable IR theories in terrorism research, the studies claim that constructivist theories are best suited to analyse how interests and identities can change with a specific time. Moreover, it is also very essential for understanding the inconsistent and uncertain responses of states towards transnational terrorism (KRISHNASWAMY, 2012).

Analysing Cyber-Security

The rise of cyber-security is now seen as a major issue of international security with the emergence of 21st century. While the conventional military issues are unrelated now, major powers are always concerned with the new agendas. However, there are still some states and scholars for whom cyber-terrorism is merely a fashionable term which is far from becoming a reality. Defining cyberterrorism as a combination of cyberspace and terrorism means it is associated not only with the hostile use of IT and action in the virtual sphere but is also characterized by all the elements of the terrorist activity (Denning, Is Cyber Terror Next?). Thus, cyberterrorism is the illegitimate use of computers, networks or technology to terrify or compel the government or people to gain certain economic, political or social benefits. Cyberterrorism is understood in two ways. According to the first concept, terrorism and cyberterrorism are distinguished only using information technology to carry out the attack, while the second focuses on computer systems as a target of attacks and not a tool to carry them out. It seems that the true definition arises only after connecting of both approaches. (Oleksiewicz, 2016). The increasing trend of terrorist organizations or lone terrorists towards the use of cyberspace is also because of the low and economical costs of cyberspace as compared to traditional military weapons. According to a report in 1998 the 30 terrorist's organisations that US State Department identified as Designated Foreign Terrorist Organisations, 12 of those 30 organizations had their own official websites and still today 33 of those groups have an official presence online. They use cyberspace not only to manipulate or destroy sensitive data but also for financial purposes or to radicalize, recruit or to spread propaganda. Former head of the US National Infrastructure Protection Centre (NIPC) Michael Vatis, has stated that "Terrorists are already using technology for sophisticated communications and fund-raising activities. As yet we haven't seen computers being used by these groups as weapons to any significant degree, but this will probably happen in the future" (Veltman 2001). In 2007 the attacks on Estonian parliament websites show that even the Article 5 of NATO and U.S. nuclear umbrella guarantees have failed to ensure the safety of the sovereignty of a nation-state within the cyberspace and how vulnerable a state's political and financial systems are in cyberspace, as at that time ENISA was also formed but still it was very difficult for NATO technical experts and European Commission to find the sources behind these attacks. Cyber-attacks on critical infrastructure can also have significantly larger effects than simpler DoS attacks and can undermine the trust of the population in their government.

From the perspective of International Relations limited amount of research has been done on cyber security and its implications in European Union. The inter-governmental nature of EU plays an interesting role with regards to cyber space as it can play a coordinating and facilitating role between the member states but due to the increased dependency of systems like voting systems, financial systems etc. on cyber space the effects of a cyber-attack in a worst case can be catastrophic. This is the reason that may be cyber security has been stated as the most important security challenge of 21st century. For example, the 2010 Stuxnet Malware that affected the Iranian Nuclear Facilities caused high damage to its nuclear plants. The Industrial Control Systems that have no connection to Internet are also at the risk of being affected by this malware. The threats along with the benefits from cyberspace have resulted in the fact that cyberspaces have moved from low politics to high politics.

High politics are involved with national security, essential institutions and decision systems that are considered critical to the state (Choucri and Clark 2012, p. 2). This is the reason that states have taken the issue of cyber security so seriously and apart from nation states international institutions like NATO, UN and EU have also developed counter strategies to overcome the threat of cyber-attack and cyber terrorism. The 2014 cyber-attacks to hack Ukrainian Presidential elections also showed that how other states or non-state actors can exploit and harm crucial data of a state for their own benefit. In order to understand the threats EU has in cyber space and the counter strategies it has opted to tackle this threat we analysed the official policy documents of EU and the agency it forms for cybersecurity but before that we will also analyse EU's counter terrorism strategy so that we could understand its implications in the domain of cyberspace.

EU Measures for Cyber Security

The EU and its Member States face many new and complicated security threats, emphasizing the need for further partnerships and collaboration among states and international institutions at all levels. Today many security threats arise from vulnerability in EU's neighbouring states and the rapidly changing shapes of use of violence, extremism and terrorism. The threat of radicalisation and terrorism is becoming transnational as it is crossing the territories and borders of states and getting diversified. To tackle these threats a unified and effective response is required from the cooperation of all EU member states and thus the European Agenda can help in assuring the coordination of states for security purposes. (MIGRATION AND HOME AFFAIRS, 2019).

EU Policy on Counter-Terrorism

The EU counter terrorism strategy involves cooperation from other states like the North America, Middle East, Western Balkans, Asia, Africa and international institutions and is based on following four pillars:

- Prevention
  To prevent the process of radicalisation and recruitment of terrorist groups by addressing its causes.

- Protection
  To reduce the vulnerability of infrastructure and citizens by protecting them from terrorist attacks.

- Pursue
  To hinder the capabilities of terrorists, EU is using strategies like the strengthening of national capabilities, the information sharing and cooperation between judiciary and police, hindering terrorist financing and depriving them of the means and support through which they carry out these activities.

- Respond
  Through this strategy EU manages, minimizes and prepares for the consequences of a terrorist attack.
  However, EU in its policy document do not address the fact that the same

> mechanism they want to be exploited can be used by others e.g. terrorists. (Ashok, 2016, n.p).

Similarly, along with the strategies made by EU in counter terrorism it took actions to secure its cyber space by passing various legislations. EU has taken several legislative actions to fight cybercrime. This includes:

- In 2013 the EU gave a command on the attacks that were directed against the information systems by asking the states to take strict measures through criminal sanctions and cyber-crime laws against large-scale attacks in cyber-space. (MIGRATION AND HOME AFFAIRS, 2019)
- In 2002 the commission gave instructions to electronic communication service providers to provide security and confidentiality to their client's private data. (MIGRATION AND HOME AFFAIRS, 2019)
- In 2001 the commission gave instructions to overcome fraud in non-cash payment methods by declaring it a crime which is punishable. (MIGRATION AND HOME AFFAIRS, 2019)
  These were some of the EU legislations to counter cyber-crime which is a way forward to help combat cyber-terrorism, for which EU has formed an agency ENISA to secure its cyberspace.

ENISA (European Union Agency for Network and Information Security)

ENISA (European Union Agency for Network and Information Security) is the EU Cybersecurity Agency created in 2004 by EU regulation. All the EU Member States and European Commission has representatives in its Management Board. The main role of Management Board is to create strategy and to cooperate to develop (and adopt) programming documents (Work Programmes). However, according to the data gathered by ENISA only 15 EU member states have actual national cyber-security strategies, the rest of the 12 states do not have staunch cyber-security strategies and that is why if they ever need to, they prefer their own national security strategies. (Sliwinski, 2014)

TFTP (Terrorist Finance Tracking Program)

Since 1970s financing of criminals has been declared as a criminal act in UK and in International law since 1999. After the incidence of 9/11 this act was taken seriously and thus the U.S. Treasury Department established TFTP (Terrorist Finance Tracking Program) after 11 September 2001 terrorist attacks which later collaborated with EU. Since then, the TFTP has provided significant intelligence to fight terrorism that has proved beneficial for both the U.S. and the States of European Union. It gives the information of transactions of terrorist finances through a secret intelligence programme SWIFT (Society for Worldwide Interbank Financial Telecommunication) which through its worldwide system of financial messaging helps in the transfer of money across global financial institutions not only to trace and detect terrorists but also their financiers. (Wesseling, 2016). However, demands are being made by EU member states to form a separate TFTP system for Europe due to the privacy concerns of Europeans as their financial data is being shared with US in bulk, so negotiations are being carried out among EU states for this purpose. The EU in collaboration with internet service providers and social media companies is trying to remove the videos and sites of jihadists rapidly. (Shea, 2018)

The treaty of Lisbon which was put into force in 2009 unified the EU strategy towards cyber-security issues. As before this treaty the EU cyber security policy was highly fragmented because there were three pillars of responsibility that were divided between European political system. These pillars were the justice and home affairs, the communities and the common foreign and security policy(CFSP). The Lisbon Treaty abolished this approach and unified it into a single strategic approach. Thus, this treaty helped to develop tools to combat cyber-crimes.

First time after about sixty years the EU is finally giving an effective policy for the security of cyber space and an advanced technique to share intelligence information, priorities of states and their security strategies, as the EU already has lost so much time in giving a strategy to protect its cyber domain, the purpose of this policy is to utilize the time effectively so that EU can now become an authentic and a better player in the domain of cyber-space. (Terzi, 2017)

EU Counter Terrorism Coordinator

According to the Council of European Union in 2007 the EU also appointed a Counter-terrorism Coordinator, Gilles de Kerchove. He was the EU High Representative for Common Foreign and Security Policy and the in charge of:

- Coordinating Council’s work on combating terrorism.
- Proposing and presenting recommendations and priorities regarding the policies to the council.
- Observing the application of EU counter-terrorism strategy.
- Keeping an outline of all EU instruments, communicating to the Council and reviewing the Council’s decisions.
- Cooperating with related preparatory bodies of the Council, the Commission and the EEAS.
- Assuring that the EU plays its significant role in combating terrorism
- Developing and enhancing the communication between EU and other countries.

CSIRT and CERT

Apart from this the EU member states also have a contract of information sharing and sudden response in case of an emergency by setting up a CSIRT network and an enhanced cyber cross-border cooperation among EU states in case of any major incident related to cyber-crime. CERT which is a Computer Emergency Response Team is also set up for handling emergency situations and risks.

Limitations in EU Measures on Cyber Security

There are some limitations on Cyber Security measures taken by EU. For example, Daesh was not a global level terrorist organization having wide ranging use of cyber space to expand its terrorist network and ideology. (Ashok, 2016, n.p) as now the increasing trend of European youth towards migration to Syria for participation in jihad is a major concern for EU, for which it is taking measures to stop the youth from taking part in this violent activity. The further involvement of educated youth in terrorist activities can increase the trend of terrorist organisations towards the use of cyber space to fulfil their agendas, as one of their agenda of recruitment is successfully working across the Europe and is the reason that youth across the Europe is migrating to Syria to join terrorist organisations. One of the major reason of use of cyber space for illegal purposes is that liberal democracies are at a disadvantage because governments have limited control over cyberspace since non-state actors are responsible for the daily function of it. The democracies must convince the non-state actors to adopt effective cybersecurity measures, where other more authoritarian states have a better ability to co-opt or coerce the non-state actors and thereby giving them an advantage in building a more secure national cyberspace (Klimburg and Tirmaa-Klaar 2011, pp. 14-19). The censorship policy on the use of internet and the limited access of individuals to deeper and darker sides of web along with the strict investigations and scrutiny by intelligence agencies can not only hinder the use of cyber space by clandestine agents but can also stop the activities of lone terrorists and terrorist organisations within the cyber space.

If we analyse cyber terrorism from the perspective of theories of International Relations than, realism has issues with handling cyberspace especially due to their state-centric understanding. Since non-state actors have gained more power due to modern information technology, this is an issue for the theory of Realism in IR. On the contrary, liberal and consructivist approaches are flexible enough to consider multilevel actors in their discourse that also include state and other actors. In a nutshell, there is need to developed a more pragmatic approach as part of middle ranged theory to be developed and explore to study such issues. (Eriksson and Giacomello 2010, pp.1-28). As cyber terrorism is a transnational crime, so it must be subjected to universal jurisdiction and that too through multinational cooperation. Moreover, cooperation of EU with US is necessary to reach to a successful point but due to the inter-governmental nature of EU it faces limitations in taking any actions regarding cyber space as the member states have a fragmented opinion about the cyber security issues. Moreover, few IR scholars believe that now EU needs to develop some other forms of cyber power and it should move from defensive approach towards offensive approach if it wants to affect a large number of cyber actors within the cyber space. However, these scholars do not explain that how EU can use offense in cyber space for its better.

Conclusion

Currently, EU has a resilience building policy which is the best way to create security, by building trust among the member states through multi-stakeholder model. EU does have a potential threat of terrorism in cyber space and it is taking measures to secure its cyber domain to provide its member states and their citizens the economic, political and national security. Several legislations have been passed by EU till date and its cooperation with other international institutions and US shows that how concerned EU is by the possible threat of cyber-terrorism in future. The EU cyber security agencies and the individual states are working at the national level according to their potential to protect their cyber space from being used by terrorists but the actions they are taking are not adequate. Moreover, there are many loopholes in EU anti-cyberterrorism policies and measures. There is a dire need for the collaboration among the public and private organisations to ensure the security of their client's personal data and the software companies also need to revise their security systems to ensure the safety of personal data of the users that is at the risk of being exploited by the terrorists due to loopholes in software company's security systems. Although, there have not been any extreme incident of cyber-terrorism which had resulted in mass killings or blood shed like the conventional incidents of terrorism, but this does not remove the threat of cyber-terrorism that many of the scholars of 21st century believes to be a reality and a future possibility.

References

[1] Ashok, I., (2016), The anatomy of a ‘Cyber Jihad’ – analysing the evolution and future of terrorism in cyberspace, in, International Business Times, 20-06-2016.

[2] Butt, S. K. (2017). Cyber Technology, Radicalization and Terrorism in. *Journal of Indian Studies*, 119-128.

[3] Clayton, M. (2014, june 17). Ukraine election narrowly avoided 'wanton destruction' from hackers. *The Christian Science Monitor*.

[4] Collingburn, A. (2016). *‘Cyber terrorism’: hyperbole or reality?* Canberra: The Strategist. (2007). *Cyberterrorism: Myth or reality?* ZDNet UK.

[5] Evan, T. (2017). *ASSESSING THE FUTURE OF CYBER TERRORISM.* Retrieved from Cambridge Judge Business School: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/170622-slides-evan.pdf

[6] Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities.* California: Stanford University.

[7] Krishnaswamy, J. (2012). How Does Terrorism Lend Itself to Constructivist Understanding? *E-International Relatons students*.

[8] Libaw, O. (2016). How Do You Define Terrorism? *abc News*.

[9] (2012). *Managing Cyber Security for Industrial Control System.* paris: ANSSI (Agence nationale de la sécurité des systèmes d’information).

[10] Max Roser, M. N. (2013, JULY). Terrorism. *ourworldindata.org*.

[11] *MIGRATION AND HOME AFFAIRS*. (2019, march 10). Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

[12] *MIGRATION AND HOME AFFAIRS.* (2019, march 20). Retrieved march 20, 2019, from European Commission: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

[13] Nielsen, A. E. (2016). *Cyberspace: opportunity or threat?* Aalborg: AALBORG UNIVERSITET.

[14] Oleksiewicz, I. (2016). Dilemmas and challenges for EU anti-cyberterrorism policy: The example of the United Kingdom. *Politechnika Rzeszowska*, 135-146.

[15] Platt, E. M. (2018). *Global Cyber Terrorism Incidents on the Rise.* New York: Marsh & Mclennan Companies.

[16] Richardson, I. L. (2011). Cyber terrorism: Menace or myth? *ResearchGate*.

[17] Schmid, A. P. (2011). *The Routledge Handbook on Terrorism Research.* USA and Canada: Routledge.

[18] Schulze, E. (2018, September 21). When this country faced a suspected Russian cyberattack – it took some big steps to stop another. *CNBC Markets*.

[19] Shea, D. J. (2018, October 08). EU takes terrorism to task with three-pronged strategy. *opinion*.

[20] Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Department of Government and International Studies*.

[21] Terzi, G. (2017). Cyber-terrorism, Cyber-Crime and Data Protection. *ICTs 17th World Summit on Counter-Terrorism.* Italy: International Institute for Counter Terrorism.

[22] Wesseling, M. (2016). *An EU Terrorist Finance Tracking System.* London: Royal United Services Institute for Defence and Security Studies.

[23] Wojciechowski, S. (2009). Why is it so Difficult to Define? *Polish Political Science Yearbook*, 58-72.

[24] Wojciechowski, S. (2009). why is it so difficult to define terrorism? *Polish Political Science Year Book.*

[25] YUNOS, Z. B. (2017, january 07). *FIC OBSERVATORY.* Retrieved from observatoire-fic.com: https://observatoire-fic.com/en/addressing-cyber-terrorism-threats-by-zahri-bin-yunos-cybersecurity-malaisia/

[26] Zerzi, M. (2017). *The Threat of Cyber Terrorism and recommendations for counter-measures.* Tunisia: Center for Applied Policy Research.