Vol.18 • 2023

ISSN. 1307 - 9190

Defence Against Terrorism Review

E-DATR

Towards a Coordinated Response to Biological Terrorism: Developing the Biological Incident Response Model
Kristen KUHN

The Nexus Between Climate Change and Terrorism and its Ramificiations in the Global South and the Global North
Zeynep SÜTALAN

Enhancing Cyber Defense and Resilience of Critical Infrastructures Against Terrorist Attacksl
Akın AYTEKİN
Mahir DURSUN

Representations of Political Violence in Digital Media: Evaluating Media Coverage of the Assassination of Japan's Former Prime Minister Shinzo Abe
Naz ALMAÇ

COE-DAT
Centre of Excellence Defence Against Terrorism

Defence Against Terrorism Review - E-DATR **ISSN 1307- 9190**

E-DATR is an international peer-reviewed journal that is abstracted and indexed in EBSCO Publishing.

E-DATR is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT). The information and views expressed in this e-journal are solely those of the lecturers and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturers are affiliated.

To cite an article in this e-journal, use the template illustrated below:
Surname, First letter of Name with a full stop (2023), The Headline of Article, Defence Against Terrorism Review (E-DATR), Vol.18., p. … - … .

Defence Against Terrorism Review - E-DATR **ISSN 1307- 9190**

DATR dergisi uluslararası hakemli bir dergidir ve EBSCO Host veritabanı tarafından taranmaktadır.

E-DATR, Terörizmle Mücadele Mükemmeliyet Merkezi Komutanlığı'nın bir yayımıdır.

NATO, TMMM K.lığı ,NATO üyesi ülkelerin ve öğretim yazarların bağlı olduğu kurumların görüş ve politikalarını temsil etmemektedir.

Bu elektronik dergiden alıntı yapmak için aşağıdaki şablonu kullanınız:
Soyadı, Adın İlk Harfi ile sonuna nokta (2023), Makalenin İngilizce Adı, Defence Against Terrorism Review (E-DATR), Vol.18., p. … - … .

Defence Against Terrorism Review
E-DATR

Vol. 18, 2023

ISSN. 1307-9190

CONTENT

The Defence Against Terrorism Review (DATR) is calling for papers for coming issues. The DATR focuses on terrorism and counterterrorism. All of the articles sent to DATR undergo a peer-review process before publication. For further information please contact datr@coedat.nato.int

Editor's Note

Dear Defence Against Terrorism Review (DATR) Readers,

Every day, acts of terrorism take on increasingly horrific shapes throughout the world, and we are all witnesses to and victims of these acts of violence. Since the spectrum of terrorism is constantly expanding, it is crucial to be able to recognize and react accordingly to all of the various strategies, tactics, and methods that terrorists utilize. To highlight other dimensions and enhance our understanding of terrorism, our DATR team proudly presents Volume 18 which features four articles covering various facets of the issue.

The issue starts with the article "Towards a Coordinated Response to Biological Terrorism: Developing the Biological Incident Response Model" by Kristen Khun, a research fellow at the Institute for Peace and Security, Coventry University, UK. Taking the readers' attention to biological occurrences like bioterrorism, Khun evaluates the necessity of a "whole society" as a coordinated response to cases like COVID-19. Khun discusses the stages of preparedness of actors both locally and internationally in such cases and touches upon the gap regarding preparedness against bioterrorism on a local level. To identify the gap, Khun suggests "the Biological Incident Response Model" which proposes a model for actors like decision-makers to act in a coordinated way on every level of a complex issue.

"The Nexus Between Climate Change and Terrorism and its Ramifications in The Global South and The Global North" is the second article in the issue by Zeynep Sütalan who is a freelance researcher. Bringing attention to climate change as a 'threat multiplier' to reveal its challenging consequences, Sütalan discusses the connection between the root causes of climate change and terrorism. On a contextual basis, the author suggests that to evaluate the effects of climate change on terrorism, specific geopolitical locations like The Global South and The Global North need to be taken into consideration. She concludes that although climate change is a global problem, the Global South suffers exceptionally from the impacts of climate change, because the states in these regions lack enough capacity to deal with the adverse effects of the climate change.

The third article in the issue is written by Akın Aytekin and Mahir Dursun, from the field of Information Security Engineering and a Professor from the Department of Electrical and Electronic Engineering, Faculty of Engineering, Gazi University, Türkiye accordingly. Named as "Enhancing Cyber Defense and Resilience of Critical Infrastructures Against Terrorist Attacks", the article argues about the dramatic impact of the destruction of critical infrastructures such as power stations or telecommunication on national security. In this context, the significance of Industrial Control Systems (ICS) in monitoring and remote control of infrastructures has been dealt with in detail in terms of Cybersecurity by comparing old systems and future directions of ICSs. Possible cyber attacks are reviewed in the light of vulnerabilities and incidents which the globe came across during last decades.

The last article of the issue is “Representations of Political Violence in Digital Media: Evaluating Media Coverage of the Assassination of Japan’s Former Prime Minister Shinzo Abe” written by Naz Almaç, a research assistant at Başkent University, Türkiye. The article focuses on diverse forms of political violence and its impact within the context of media and terrorism. Adopting the communication perspective framing theory, Almaç investigates how political violence is framed and circulated through digital media, and how media firms utilize rhetorical strategies grounded on binary oppositions to influence their audience. In this sense, Almaç chooses a specific case of the assassination of Japan’s former Prime Minister Shinzo Abe in digital media to apply the discussed theories and to examine the influence of digital media on terrorism from different perspectives such as East and West. The article compared how different news sources frame the same events or issues.

As the DATR team, we would like to thank all authors for the contributions they have made to this issue and the reviewers for their thoughtful and caring comments and efforts toward improving our manuscript. DATR always welcomes and encourages contributions from experts, civil and military officers as well as academics to send us their comments, suggestions, and rewarding work on defense against terrorism.

We sincerely hope you find the information in this issue rewarding, and we hope to see you in the upcoming issues.

Sincerely yours,
Uğur Güngör
Editor-in-Chief

Defence Against Terrorism
Review DATR Magazine

E-DATR, 2023; 18 : 7-26
Electronic Online ISSN 1307 - 9190
https://dergipark.org.tr/tr/pub/datr

Towards a Coordinated Response to Biological Terrorism: Developing the Biological Incident Response Model

Kristen Kuhn[1]

Abstract

Since 9/11, a significant body of research has been developed to address initiatives enacted to respond to biological incidents, including bioterrorism, with most of these efforts being made at the national and institutional levels. The COVID-19 global pandemic has, however, underlined the importance of a coordinated response to bioterrorism that emphasizes a 'whole of society' approach in its delivery and, as such, it is fundamental that new insights inform how actors can enhance their preparedness. A first stage for these actors must be an understanding of their unique roles for reducing the vulnerability of and the response to biological incidents. Yet, despite research indicating that local authorities are particularly vulnerable, little attention is given to planning for bioterrorism at this level. This study makes a step towards addressing this gap by developing an understanding of where different actors can best focus their efforts to prepare for biological incidents and develops the Biological Incident Response Model. The premise is that proposing a model to understand the roles of actors, rather than one that seeks to establish benchmarks for collective security, can help decision-makers to recognize their responsibility in a coordinated response to complex issues where no

[1] Kristen Kuhn, Research Fellow, Institute for Peace and Security, Coventry University, CV1 2TL, United Kingdom, kristen.kuhn@coventry.ac.uk (K. Kuhn) ORCID(s):0000-0001-8906-0197 (K. Kuhn)

one actor can advance alone. This approach creates a greater sense of ownership at each level to enhance coordination and improve response.

Keywords: *Bioterrorism, Counter-terrorism, Decision-making, Protective security, Security governance*

1. Introduction

A new kind of biological anxiety was among the fears that sprung from the September 11, 2001 terrorist attacks (9/11), which resulted from the long-term biological effects of 9/11 and a series of ensuing bioterrorism attacks.[2] According to Garrett, these new attacks were initiated by an anthrax-infected letter posted in the United States, just eight days after 9/11, which served as a harbinger to a long chain of such attacks which led to death and widespread global hysteria. When the postal center at the White House received mail infected with anthrax in October 2001, former U.S. President Bush sought to quell national sentiment when he told the nation, "I don't have anthrax. . .. I'm confident that when I come to work tomorrow that I'll be safe"[3]. This sentiment was however captured on the international stage just over a year later at the 2002 Prague Summit, where former NATO Secretary General Lord Robertson stated that "September 11, 2001 and its aftermath confronted the whole world with new challenges. A deadly cocktail of threats is now menacing free societies".[4] At the summit, heads of state and government at NATO launched five initiatives[5] to strengthen the Alliance's capability to deter and defend against nuclear, biological and chemical (NBC) weapons. Among other things, these initiatives recognize that while it is impossible to prevent all bioterrorism attacks, such risks must be managed collaboratively to protect from and prepare for such attacks in the future, enabling people to go about their lives freely and with confidence.

---

2 Garrett, L. (2021). The Forgotten Biological Terror of 9/11. *Foreign Policy*, available at https://foreignpolicy.com/2021/09/10/ the-forgotten-biological-terror-of-9-11/

3 Remarks by the President in Photo Opportunity with Members of Congress, The Cabinet Room. (2001). President Says Terrorists Won't Change American Way of Life. *Office of the Press Secretary*, available at https://georgewbush-whitehouse.archives.gov/news/ releases/2001/10/text/20011023-33.html

4 Heads of State and Government. (2002). Press Release (2002)127: Prague Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague. *NATO*, available at https://www.nato.int/docu/0211prague/ speeches-e.pdf

5 These initiatives included: a Prototype Deployable NBC Analytical Laboratory; a Prototype NBC Event Response team; a virtual Centre of Excellence for NBC Weapons Defence; a NATO Biological and Chemical Defence Stockpile; and a Disease Surveillance system.

Given the persistent and evolving approach to countering terrorism since 9/11, it is no surprise that a significant body of research has been developed to address efforts enacted to increase the situational awareness, capabilities across domains and multilateral initiatives which respond to biological incidents, including bioterrorism, with most of these efforts made at the national and institutional levels.[6] The role of local authorities in responding to bioterrorism incidents has received much less scholarly attention in comparison to other actors where significant funding has been made available for countering terrorism. The global COVID-19 pandemic has, however, exposed and heightened significant vulnerabilities to biological warfare (biowarfare)[7] and thus it has acted as a catalyst for greater emphasis on a coordinated response to biological threats as laws, put forward by diverse actors, proposed legislation to provide better protection from biological threats (including bioterrorism) in public venues. However, as of May 2023, no legislation regarding how to respond to biological threats has been brought forward at the local level, nor have subsequent consultations been launched by governments to evaluate the response to such threats. Sporadic research on analyzing response to pandemic, lesson-learned, recommendations[8] and exploring how things like digital behavior[9] and commuter behavior[10] have changed because of the pandemic, suggests there is an opportunity to reflect and improve. This highlights how unprepared the world was, collectively, to deal with a biological threat and the ambiguity around which actors are responsible (and accountable) for the response.

In the same vein as biological threats like the COVID-19 pandemic, response to bioterrorism must place emphasis on a 'whole of society' approach in its delivery and, as such, it is fundamental that new understandings, evidence and insights inform how to best protect from bioterrorism and how actors can enhance their preparedness. The success of efforts to counter bioterrorism depend on how protective security and preparedness measures introduced by diverse actors such as local authorities, national authorities, and international bodies are enacted on the ground. A first

---

6 Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

7 Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

8 Ibid.

9 Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). Covid-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs*, 1–22.

10 Harrington, D. M., & Hadjiconstantinou, M. (2022). Changes in commuting behaviours in response to the covid-19 pandemic in the uk. *Journal of transport & health*, *24*, 101313.

stage for these actors must be an understanding of their unique roles for reducing vulnerability to bioterrorism attacks and responding to such threats.

While actors like the U.S. President and the NATO Secretary General- and the nations and institutions they represent- play a key role in responding to bioterrorism threats, they are not solely responsible. Indeed, international and national emergencies often begin as local incidents, which escalate for reasons including insufficient planning and preparedness. This holds particularly true for the case of biological threats, where most threats are discovered for the first time by a doctor in a hospital.[11] Yet, despite research indicating that local hospitals are particularly vulnerable, little effort is made when it comes to planning for terrorism at this level.[12] This research makes a step towards addressing that gap by developing an understanding of where different actors can best focus their efforts to prepare for a bioterrorism incident. This is done by first reviewing the roles of diverse actors in a response, which then underpins the development of the Biological Incident Response Model to identify the key responsibilities of actors in responding to a bioterrorism attack. The premise for this is that developing a model for understanding the roles of actors, rather than one that seeks to establish collective benchmarks for security measures that are already in place and what needs to be improved, can help decision-makers to recognize their unique position in achieving a sense of coordinated preparedness to respond to issues where no one actor can advance alone. This approach creates a greater sense of ownership at every level, which may enhance coordination to improve response.

In terms of limitations, this study did not include the resources to conduct a baseline investigation of roles in local and national authorities, as well as international organizations and therefore had to rely on theoretical considerations and the author's knowledge of security governance. Validation (piloting and evaluation) with each of these groups is important before the model is operationalized, to ensure its validity and reliability, as it is fundamentally based on a theoretical construct.

In what follows, a description is provided on how the proposed model has been developed and the roles of different actors are reviewed (Section 2). The Biological Incident Response Model is then presented (Section 3). The final section provides conclusions from the research (Section 4).

[11] Alexander, G. C., & Wynia, M. K. (2003). Ready and willing? physicians' sense of preparedness for bioterrorism. *Health Affairs*, *22*(5), 189–197.

[12] Perry, R. W., & Mankin, L. D. (2005). Preparing for the unthinkable: Managers, terrorism and the HRM function. *Public Personnel Management*, *34*(2), 175–193.

2. Background

The threat of bioterrorism is not new to global security. Indeed, terrorist groups have made use of weaponized biological agents for many years, and this remains a growing concern.[13] While biological weapons possess a deadly potential, their actual utilization is infrequent and typically on a small scale.[14] The COVID-19 pandemic has, however, emphasized the growing importance of taking a comprehensive approach to understanding biological vulnerabilities and assessing biological threats.[15] NATO, for instance, has expressed an intent to address bioterrorism in the post-COVID-19 world and security will increase as indicated by recent efforts to strengthen the Alliance's awareness, capabilities and engagements.[16] From a review of existing literature, a number of themes emerged in relation to the types of methods used for understanding coordination (Section 2.1) and the key actors who play a role in managing preparedness methods for countering bioterrorism threats (Section 2.2).

COVID-19 exhibits several traits of an optimal biological weapon, such as a high transmission rate, prolonged incubation period, airborne transmission, and substantial morbidity/mortality.[17] Indeed, during the early stages of the pandemic, there were suspicions that the virus was being engineered as a biological weapon in a laboratory in Wuhan, China.[18] While these allegations have been dismissed as conspiracy theories stemming from misinformation campaigns, the resulting pandemic and the ensuing public panic bear resemblances to the aftermath of a bioterrorism attack.[19] "The wide-reaching and disruptive consequences of the pandemic challenge the ability of national governments, public health authorities,

---

13 Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

14 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

15 Alleslev, L. (2021). Biological threats: Technological progress and the spectre of bioterrorism in the post-covid-19 era. *NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technological Trends and Security (STCTTS)* , available at https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/024%20STCTTS%2021%20E%20rev%201%20fin%20-%20%20BIOLOGICAL%20THREATS%20-%20ALLESLEV.pdf

16 Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

17 Chen, Y., & Li, L. (2020). Sars-cov-2: virus dynamics and host response. *The Lancet Infectious Diseases*, *20*(5), 515

18 BBC Monitoring and UGC Newsgathering. (2020). *BBC Monitoring: China coronavirus: misinformation spreads online*, available at https:// www.bbc.com/news/blogs-trending-51271037

19 Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

medical services, and international organizations to respond effectively."[20] The events unfolding in the United States during the 2019 COVID-19 pandemic shaped a global narrative on how to address a biological crisis.[21] If COVID-19, a huge public health issue, has encouraged decision-makers to consider biological threats, then it makes sense to investigate bioterrorism through the perspective of public health. However, where epidemiology furnishes evidence-based insights into the distribution of health effects and their associated risk factors among diverse population groups, it may neglect the reality that decision-making relies not only on scientific evidence but also on political, economic, and social factors.[22] This study includes reworking tools native to the field of epidemiology for use in a novel way that is both practical and 'fit for purpose' in that it adds much-needed structure to a vital dialogue among diverse stakeholders and decision-makers who each play a distinct role in countering bioterrorism. This interdisciplinary study investigates models related to disease causation and management, to explore parallels which may be used to further an understanding of how biological threats can be managed collaboratively.

This research is focused on investigating how actors can coordinate a response to a bioterrorism attack, however it acknowledges that attack types, methods and rationales are not linear, and can evolve as a result of many factors, including environmental conditions, protective measures and capabilities.[23] Further, while previous research[24] is concerned with discerning between intentional and naturally occurring infectious disease outbreaks, this research adopts a protective security approach and suggests that both intentional and naturally occurring disease outbreaks require the same immediate response, so there is no need to distinguish between them from a decision-making perspective. Consider that in the immediate aftermath of such an attack, it is highly unlikely that executive decision-makers

---

20 Alleslev, L. (2021). Biological threats: Technological progress and the spectre of bioterrorism in the post-covid-19 era. *NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technological Trends and Security (STCTTS)* , available at https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/024%20STCTTS%2021%20E%20rev%201%20fin%20-%20%20BIOLOGICAL%20THREATS%20-%20ALLESLEV.pdf

21 Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

22 Gulis, G., & Fujino, Y. (2015). Epidemiology, population health, and health impact assessment. *Journal of epidemiology*, *25*(3), 179–180.

23 Marchment, Z., & Gill, P. (2022). Spatial decision making of terrorist target selection: Introducing the track framework. *Studies in Conflict & Terrorism*, *45*(10), 862–880.

24 Dembek, Z. F., Kortepeter, M. G., & Pavlin, J. A. (2007). Discernment between deliberate and natural infectious disease outbreaks. *Epidemiology & Infection*, *135*(3), 353–371.

have enough information to assess where the threat originates. For instance, one study[25] presents three separate cases of bioterrorism events in the United States- all of which were not immediately identified as deliberate. Therefore, to establish the scope and focus for the model, less emphasis was placed on the specific threat types and threat actors themselves and instead focus was on building an understanding of the role of local, national, and international actors if an attack occurred. This study considers three categories of epidemiological cases, including: intentionally caused epidemics, an unintentional release of a biowarfare agent, and naturally occurring outbreaks that mimic bioterrorism.[26] This is because all incidents provide insights into how biological incidents are managed and may improve future response.

The Epidemiological Triangle

Several models of disease causation and transmission have been identified in literature.[27] Among these is the epidemiological triangle, the traditional model for infectious disease, seen in Figure 1. Epidemiology is a field that plays a vital role in characterizing health status, pinpointing risk factors, and examining connections between health and potentially harmful agents.[28] As stated by Gulis and Fujino (2015), in this this model, disease arises from the interplay between the agent and a susceptible host within an environment conducive to the transmission of the agent from a source to that host. Agent, host, and environmental factors intertwine in various complex ways to generate disease. The specific nature of different diseases necessitates unique balances and interactions among these three components.

In its original context, the 'agent' pertains to an infectious microorganism or pathogen, encompassing viruses, bacteria, parasites, or other microbes. Typically,

---

25 Ibid.

26 Ibid.

27 Thompson, K. M. (2016). Evolution and use of dynamic transmission models for measles and rubella risk and policy analysis. *Risk Analysis*, *36*(7), 1383–1403; Riley, S. (2007). Large-scale spatial-transmission models of infectious disease. *Science*, *316*(5829), 1298–1301; Rothman, K. J. (1976). Causes. *American journal of epidemiology*, *104*(6), 587–592; Koopman, J. (2004). Modeling infection transmission. *Annu. Rev. Public Health*, *25*, 303–326; Barbour, A. D. (1978). Macdonald's model and the transmission of bilharzia. *Transactions of the Royal Society of Tropical Medicine and Hygiene*, *72*(1), 6–15; Kiss, I. Z., Berthouze, L., Taylor, T. J., & Simon, P. L. (2012). Modelling approaches for simple dynamic networks and applications to disease transmission models. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *468*(2141), 1332–1355.

28 Gulis, G., & Fujino, Y. (2015). Epidemiology, population health, and health impact assessment. *Journal of epidemiology*, *25*(3), 179–180.

the presence of the agent is necessary for disease to occur; however, the mere presence of the agent alone is not always enough to cause the disease. Various factors determine whether exposure to an organism will lead to disease, including the organism's pathogenicity and the dose. Over time, the concept of the agent has expanded to encompass chemical and physical causes of disease or injury, such as the L-tryptophan contaminant responsible for eosinophilia-myalgia syndrome or repetitive mechanical forces linked to carpal tunnel syndrome.

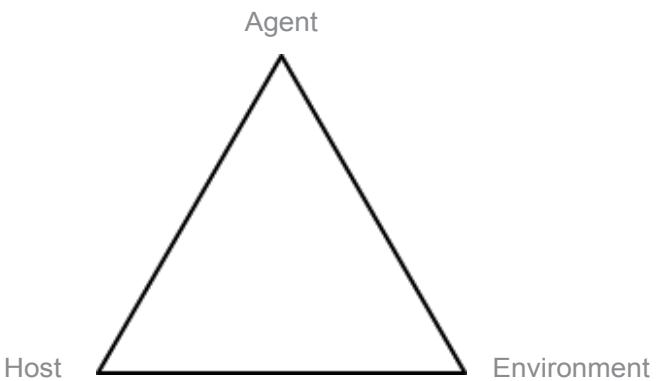

Figure 1: The epidemiological triangle **Source:** https://www.cdc.gov/csels/dsepd/ss1978/lesson1/section8.html

In the context of this study, the term 'host' pertains to the human susceptible to the disease. Various intrinsic factors, often referred to as risk factors, can impact an individual's exposure, susceptibility, or response to a causative agent. Behaviors like sexual practices, hygiene, and personal choices, along with demographic factors like age and sex, often influence opportunities for exposure. Susceptibility and response to an agent are shaped by factors such as genetic makeup, nutritional and immunological status, anatomical structure, and the presence of diseases or medications. On the other hand, the 'environment' encompasses extrinsic factors influencing the agent and the likelihood of exposure. Environmental factors include physical elements like geology and climate, biological aspects such as insects transmitting the agent, and socio-economic factors like crowding, sanitation, and the availability of health services. It is essential to understand the environment in its broadest sense, encompassing social, economic, cultural, political, and physical dimensions, all of which are pertinent and relevant.[29]

[29] Gulis, G., & Fujino, Y. (2015). Epidemiology, population health, and health impact assessment. *Journal of epidemiology*, *25*(3), 179–180.

The epidemiological triangle serves as a valuable model for understanding many diseases; however, it is not suitable for diseases that have multiple contributing causes without a single necessary one, such as cardiovascular disease or cancer. However, this limitation does not apply to issues of bioterrorism where there is often one identified threat vector. Another challenge associated with this model is that it is used inconsistently in the literature, with one model depicting the agent, host, and environment as exerting equal influence. (as seen in Figure 1) which another model by the same name depicts the agent and host as interdependent variables influenced by the environment.[30] For this study, what is important is to emphasize the interplay between these three elements, rather than their weight or the exact nature of their interrelationships. For this reason, the simplest form of the triangle is depicted, while the author acknowledges that various diseases necessitate distinct balances and interactions among these three components. However, any model which that illustrates agent, host, and environmental factors interrelating in various ways to generate disease is considered an epidemiological triangle in this study.

Although epidemiology has a rich tradition and has amassed a wealth of experience in evaluating micro-environments and specific agents that may affect health, it has been seldom utilized to assess public health issues at the policy or strategic level.[31] As this study points out, epidemiology alone is not equipped to facilitate dialogue among stakeholders within its scientific discipline which may explain its infrequent use. Nevertheless, to enhance a population's health status the insights generated by epidemiology need to be translated into practical interventions.[32] Designing effective public health measures to control or prevent disease usually involves assessing all three components and understanding their interactions.

2.2. Actors in a Coordinated Response to Bioterrorism

Different types of interventions exist to address all three elements of the epidemiological triangle.[33] Coordination is a vital factor of preparedness in the context of responding to biological incidents, as emphasized by Gulis and Fujino

---

30 Centers for Disease Control and Prevention. (2012). *Lesson 1: Introduction to Epidemiology*, available at https://www.cdc.gov/csels/ dsepd/ss1978/lesson1/section8.html

31 Gulis, G., & Fujino, Y. (2015). Epidemiology, population health, and health impact assessment. *Journal of epidemiology*, *25*(3), 179–180.

32 Ibid.

33 Ibid.

(2015) when they state, “the health of populations depends on many different factors”. Here, coordination refers to the ability of actors to clearly implement decisions in relation to roles, responsibility, and resources. This study acknowledges the role of diverse actors in responding to such an incident, where response may also require the inclusion of non-traditional actors for investigating disease and managing outbreaks.[34] However, given the exploratory nature and limited scope of this study, which aims to develop a conceptual model, three main actor groups are presented: international bodies, national and local authorities.

2.2.1. International Bodies

The risk of bioterrorism underscores the importance of establishing effective biodefense strategies and the strengthening of global governance frameworks related to arms control and biosecurity.[35] In relation to how international bodies interact with the environment, they are often responsible for managing norms, coordinating information and intelligence, and carrying out situational threat analysis on a societal scale to ensure effective biodefence strategies. Previous research[36] suggests that NATO’s recent responses to terrorist and chemical attacks, epidemics and the COVID-19 pandemic exemplify the Alliance’s role in upholding collective biodefence and deterrence. While the concepts of defense and deterrence are commonly associated with nuclear warfare, they can also be applied to characterize biowarfare.[37] Deterrence, in this case, may include vaccines and preventative measures to mitigate susceptibility to a microbe.[38]

In terms of how international bodies interact with the agent, they play a vital role in the governance of biosafety and biosecurity.[39] They can strengthen international governance frameworks and are poised to help build global resilience and

---

[34] Dembek, Z. F., Kortepeter, M. G., & Pavlin, J. A. (2007). Discernment between deliberate and natural infectious disease outbreaks. *Epidemiology & Infection*, *135*(3), 353–371.

[35] Alleslev, L. (2021). Biological threats: Technological progress and the spectre of bioterrorism in the post-covid-19 era. *NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technological Trends and Security (STCTTS)* , available at https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/024%20STCTTS%2021%20E%20rev%201%20fin%20-%20%20BIOLOGICAL%20THREATS%20-%20ALLESLEV.pdf

[36] Iftimie, I. A. (2020). The implications of covid-19 for nato’s counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

[37] Snyder, G. H. (2015). *Deterrence and defense* (Vol. 2168). Princeton University Press.

[38] Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

[39] Koblentz, G. D., Lentzos, F., Houser, R., Ameneiros, M., Earnhardt, B., Rodgers, J., & Wingo, H. (2023). *Global BioLabsReport2023*, available at https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/ 1678955285754/KCL0680_BioLabs+Report_Digital.pdf

enforce agreed upon standards. This includes, for example, the "Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction" (BTWC).[40] At present, NATO member countries do not have biological weapons programs, yet they actively engage in defensive research on biological agents and consistently allocate resources to ensure biological defense capabilities.[41] Moreover, within NATO, Allies have established baseline requirements for national resilience.[42] However, although biowarfare is regarded as a "weapon of mass destruction" and is prohibited under the treaty, not all actors and adversaries adhere to these standards. Consider that, since 1945, only six countries have publicly acknowledged developing biological weapons although there is sufficient evidence to suspect over a dozen.[43] Further, terrorist groups and covert operations, often ineligible or unwilling to ratify the treaty, have at times utilized biological weapons for smaller-scale operations.[44] Another challenge to upholding such standards is that biological weapons provide deniability as their attacks can mimic natural outbreaks, making attribution challenging.[45]

2.2.2. National Authorities

National authorities bear the primary responsibility to protect their populations and critical infrastructure against bioterrorism attacks.[46] Biowarfare is an unlikely but significant threat for military operations and national security.[47] A pressing concern today is whether progress in biotechnology might entice states to revive historical

---

40 United Nations. (1972). *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, available at https://legal.un.org/avl/ha/cpdpsbbtwd/cpdpsbbtwd.html

41 Alleslev, L. (2021). Biological threats: Technological progress and the spectre of bioterrorism in the post-covid-19 era. *NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technological Trends and Security (STCTTS)* , available at https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/024%20STCTTS%2021%20E%20rev%201%20fin%20-%20%20BIOLOGICAL%20THREATS%20-%20ALLESLEV.pdf

42 North Atlantic Treaty Organization. (2022). *Weapons of mass destruction*, available at https://www.nato.int/cps/en/natohq/topics_50325.htm

43 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

44 Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

45 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

46 North Atlantic Treaty Organization. (2022). *Weapons of mass destruction*, available at https://www.nato.int/cps/en/natohq/topics_50325.htm

47 Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

biological weapons programs or initiate new ones.[48] Charlet (2018) suggests that such an outcome would significantly erode the progress made in recent decades and could instigate new conflicts or reignite past arms races, thereby destabilizing the international order.

In terms of how national authorities interact with the host, they are responsible for protecting their populations. Prior research[49] states that, within NATO member states, the protection of civilians from biological agents and bioterrorism is a national responsibility. This has historically included the development of advanced biological weapons programs for the purpose of deterrence, as was started by the United States in 1942 and stopped in 1969 due in part to uncertainties as to its contribution to national security.[50] This also includes strategic communications and safeguarding. In terms of the present biotechnology revolution, Charlet (2018) asserts that succumbing to fear-mongering or excessive regulation could undermine the almost unimaginable benefits of such technology, but neglecting to foresee and address substantial risks, such as the resurgence of state biological weapons programs, would be equally problematic.

In terms of how national authorities interact with the environment, they have a responsibility to protect their territories, critical infrastructure, and assets.[51] Iftimie (2020) highlights that, within the context of NATO, member states lead in targeting bioterrorism entities within their own territories. This may take the form of installing temporary spatial or territorial rules such as border controls, lockdowns, curfews. It may also take the form of enforcing societal barriers such as social distancing or regulation around crowded places.

Any public space where mass gatherings take place or critical infrastructure vital for the smooth functioning of society exists represents a potential target for bioterrorism attacks.[52] Christian (2013) highlights that not only do hospitals and academic health centers fit this profile, but the latter faces an elevated risk as they can serve as potential sources of agents of opportunity. Furthermore, facilities

---

48 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

49 Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

50 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

51 Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

52 Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

housing potentially hazardous bacteria, toxins, or viruses are often surprisingly ill-secured, increasing the risk of theft, accidents, or leaks.[53] These may be referred to as biosafety-level-3 (BSL3) or BSL4 labs, as seen in Figure 2. As of December 2023, there are 51 operational BSL4 labs, three under construction, and fifteen in the planning stages- across 27 countries.[54] According to Koblentz et al. (2023), around 75 percent of currently operational BSL4 labs are situated in urban areas, where dense populations could worsen the consequences of an accidental release. The global number of BSL4 labs has consistently risen since the 2001 anthrax letter attacks in the United States, and the COVID-19 pandemic has prompted another swift escalation in the construction of BSL4 labs.[55] According to Global Biolabs (2023), since the onset of the pandemic, nine countries have declared intentions to construct twelve new BSL4 labs.

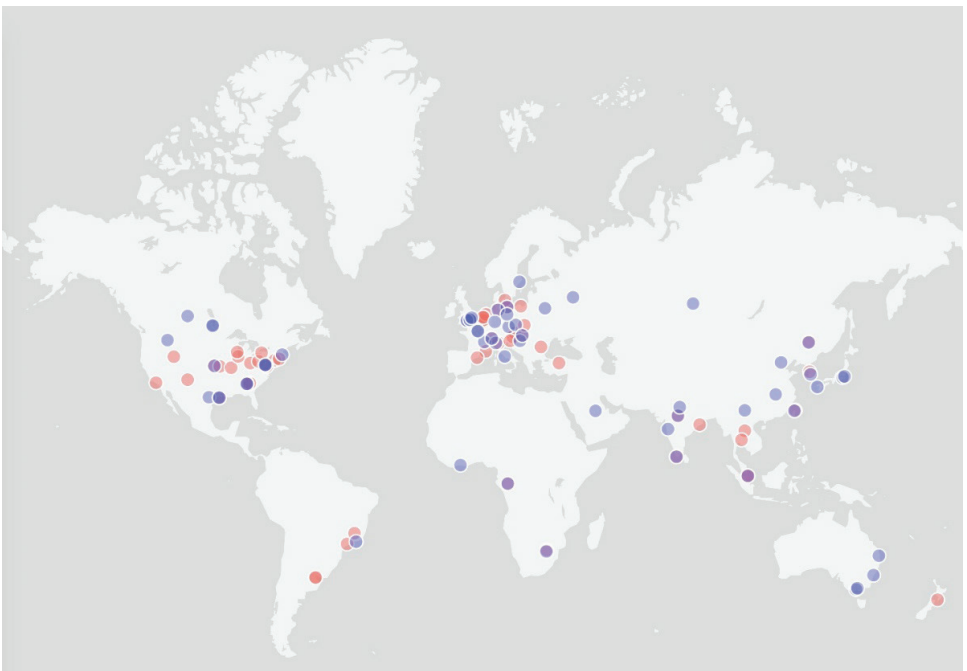

Figure 2: BSL4 (blue) and BSL3+ (red) labs around the world (2023)
Source: https://www.globalbiolabs.org/map

[53] Jenkins, B. (2017). The global health security agenda and the role of the world organisation for animal health. *Revue Scientifique et Technique (International Office of Epizootics)*, *36*(2), 639–645.

[54] Koblentz, G. D., Lentzos, F., Houser, R., Ameneiros, M., Earnhardt, B., Rodgers, J., & Wingo, H. (2023). *GlobalBioLabsReport2023*, available at https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf

[55] Ibid.

2.2.3. Local Authorities

A local authority is an officially designated organization responsible for overseeing all public services and facilities within a specific geographical area. Local authorities have the first line of official public responsibility[56] and are a key piece in a larger arrangement needed for effective counter terrorism. As such, they must be supported by a strategic vision, adequate resources, and a well-defined legal framework.[57]

In terms of bioterrorism, one of the key responsibilities of local authorities is recognition of the agent. Recognition of a bioterrorism incident involves two components: (1) distinguishing that an outbreak of multiple cases of illness is intentional rather than natural, and (2) identifying the specific organism or agent causing the illness.[58] The identification of a bioterrorism event is the most challenging part of the response.[59] The effective control of infectious disease transmission in a population, whether natural or intentionally induced, is closely tied to the prompt recognition of the event.[60] Critical care physicians wield significant influence in identifying and responding to a bioterrorism attack, necessitating their familiarity with the diagnosis and management of the most probable bioterrorism agents.[61] Furthermore, public health authorities should be made aware of intentional outbreaks of biological agents.[62] Effective response to such an outbreak necessitates collaboration between clinicians and public health officials.[63]

Another key responsibility of local authorities is to mitigate risk for community members (the host) by taking protective measures, including for example enforcing social distancing measures in the case of COVID-19. Target populations can be protected by vaccines and other prevention measures.[64] While this role of local

---

56 McLoughlin, D. (1985). A framework for integrated emergency management. *Public administration review*, *45*, 165–172.

57 Vidino, L., & Hughes, S. (2015). Countering violent extremism in America. *The George Washington University Center for Cyber Homeland*.

58 Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

59 Radosavljevic, V., & Belojevic, G. (2012). Unusual epidemic events: a new method of early orientation and differentiation between natural and deliberate epidemics. *Public Health*, *126*(1), 77–81.

60 Dembek, Z. F., Kortepeter, M. G., & Pavlin, J. A. (2007). Discernment between deliberate and natural infectious disease outbreaks. *Epidemiology & Infection*, *135*(3), 353–371.

61 Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

62 Dembek, Z. F., Kortepeter, M. G., & Pavlin, J. A. (2007). Discernment between deliberate and natural infectious disease outbreaks. *Epidemiology & Infection*, *135*(3), 353–371.

63 Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

64 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

authorities is often overlooked in literature and policy about counterterrorism, it is well established. For instance, local authorities in Britain have their origins in organizations established by the UK government during the first half of the nineteenth century in response to cholera epidemics, where their role was to provide clean water supplies, ensure cleaner streets, enhance sanitation, and regulate slaughterhouses.[65] Critical care clinicians must also be equipped to handle mass casualty situations.[66]

3. The Biological Incident Response Model

The review of literature, including the epidemiological triangle (Section 2.1) and the evaluation of the roles of diverse actors in a coordinated response (Section 2.2), underpins the development of the Biological Incident Response Model, seen in Figure 3. This model serves as a foundation for the development of a collaborative counterterrorism method to enhance the awareness of actors in delivering their bioterrorism incident responsibilities.

Central to this research is the introduction of a model that enables different actors to understand the responsibilities of their security preparedness and protective responses in relation to other actors. Existing literature was reviewed to identify common themes characteristic to each role. It is worth noting that no reviewed source covered protection from all actors relevant to bioterrorism threats, and most existing sources were focused on specific security considerations such as the role of technology in bioterrorism. The author therefore made judgements about the applicability of such features to existing roles, discarding some as irrelevant and assuming others were relevant to multiple actors, based on her knowledge of international and government structures. Given that there are a wide range of actor contexts that need to be considered within the model, the author reasoned the model should be kept general. Three groups (local, national, international) were the smallest number that would account for this variety and range. These three groups were selected on the basis that such actors cover a vast range of decision-making bodies.

---

[65] Islington Council. (2023). *The role of local authorities*, available at https://www.islington.gov.uk/about-the-council/ who-we-are/how-the-council-works/the-role-of-a-local-authority#:~:text=They%20represent%20their%20local% 20communities,priorities%20and%20 provide%20community%20leadership.

[66] Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

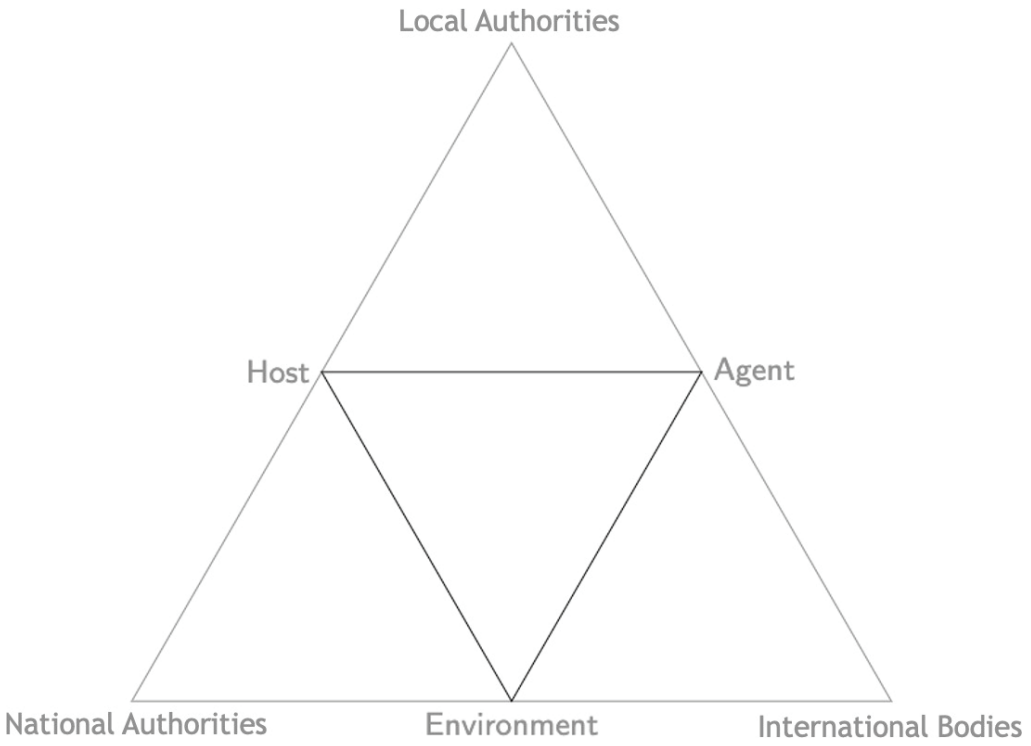

Figure 3: The Biological Incident Response Model, which includes an inverted version of the epidemiological triangle and implementation bodies

Each of the three identified groups were aligned to two angles of the epidemiological triangle (forming three additional triangles), as was consistent with the analysis of responsibilities for each in the literature in relation to the agent, host and environment (see Section 2.2). This is not to say that if the national authorities are best posed to manage strategic communications, other actors should not make efforts in this area. However, by separating out key roles, this model can help to identify responsibilities which may facilitate a dialogue (which must be on-going due to the evolving nature of biological threats) on how efforts to counter biological terrorism can be coordinated amongst actors, as opposed to efforts being disregarded or even duplicated.

4. Conclusion

Bioweapons have a historical precedent spanning centuries and the specter of bioterrorism remains a persistent future risk.[67] On any given day, citizens could be quickly overwhelmed by a bioterrorism attack or coordinated attacks undertaken during a biowarfare campaign, which employ(s) an array of novel forms to exact harm and fear. Developing an understanding of response at international, national, and local levels is vital as it can help to improve activities to be reconstituted after a major attack, to ultimately save lives.[68] This study addressed a gap identified where little attention has been paid to preparing for and protecting against bioterrorism at the local level and includes three main contributions. First, it reviewed models for disease causation within the realm of public health, and it also reviewed the relevant actors in a response to a biological incident. From this review, it determined local authorities and doctors to be vital actors in the coordinated response to biological incidents, alongside national authorities, and international bodies. Second, it developed the Biological Incident Response Model and proposed this as a new preparedness tool to coordinate response actors. This may improve upon the preparedness methods which empower authorities at all levels to play an active role in countering bioterrorism. Third, this study may enhance ownership and dialogue around a coordinated response to bioterrorism incidents.

While intentional large-scale bioterrorism attacks, especially by adversarial nation-states, have not occurred to date, there is no guarantee that this trend will persist in the future.[69] Indeed, the adverse social and economic repercussions of the COVID-19 pandemic may fuel a growing intent by terrorist groups to employ biological agents against NATO member states to fulfil their goals.[70] In April 2020, the UN Secretary-General Antonio Guterres warned that "the weaknesses and lack of preparedness exposed by this pandemic provide a window into how a bioterrorist attack might unfold – and may increase its risks"[71]. COVID-19 highlights the importance of improved preparedness against all kinds of public health threats,

---

67 Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

68 Sloan, S. (2002). Meeting the terrorist threat: The localization of counter terrorism intelligence. *Police Practice and Research*, *3*(4), 337–345.

69 Riley, S. (2007). Large-scale spatial-transmission models of infectious disease.*Science*, *316*(5829), 1298-1301.

70 Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

71 Clarke, G. (2020). *COVID-19 threatening global peace and security, UN chief warns.* UN News, available at https://news.un.org/en/ story/2020/04/1061502

including bioterrorism.[72] Thus, actors must improve their ability to identify and respond to such attacks.[73] Ultimately, the Biological Incident Response Model aims to support actors in protecting against bioterrorism and to ensure they are properly prepared in the case of such an incident. While the proposed model does not offer a single answer to an enduring security threat, it aims to draw on insights from past events to increase the capacity and capability to manage risks and response effectively through means of clear and improved communication. Strategically allocated resources and effective leadership may save lives by facilitating swift responses to outbreaks, thereby mitigating the impact of a biological agent- even in the absence of an intentional attack.[74]

While the development of the Biological Incident Response Model is conceptual in nature, a clear direction for future work includes testing and validation. In terms of testing, the model may be used to analyze the roles of actors in actual (or imagined) bioterrorism attacks, to generate insights about coordination in response. This could be extended to explore the incorporation of new actors through the survey of additional literature, or to explore the use of the model for other nuclear, biological and chemical (NBC) incidents or pandemics, as well as futuristic scenarios with new threats, to explore the limits of its application. While the proposed model is focused on responding to bioterrorism attacks, it has applicability and interoperability across actor groups who wish to improve their understanding of various roles regarding of preparedness and responsibility for responding to a bioterrorism incident. In terms of validation, this includes having actors from each identified group engage with the model and to validate its design by both assessing whether the coordinating roles identified in the literature reflect their own realities and suggesting shifts in roles and responsibilities to incorporate emerging threats.

---

72 Alleslev, L. (2021). Biological threats: Technological progress and the spectre of bioterrorism in the post-covid-19 era. *NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technological Trends and Security (STCTTS)* , available at https://www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/024%20STCTTS%2021%20E%20rev%201%20fin%20-%20%20BIOLOGICAL%20THREATS%20-%20ALLESLEV.pdf

73 Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

74 Ibid.

References

Alexander, G. C., & Wynia, M. K. (2003). Ready and willing? physicians' sense of preparedness for bioterrorism. *Health Affairs*, *22*(5), 189–197.

Alleslev, L. (2021). Biological threats: Technological progress and the spectre of bioterrorism in the post-covid-19 era. *NATO Parliamentary Assembly, Science and Technology Committee (STC), Sub-Committee on Technological Trends and Security (STCTTS)* , available at https:// www.nato-pa.int/download-file?filename=/sites/default/files/2021-10/024%20STCTTS%20 21%20E%20rev%201%20fin%20-%20%20BIOLOGICAL%20THREATS%20-%20ALLESLEV.pdf

Barbour, A. D. (1978). Macdonald's model and the transmission of bilharzia. *Transactions of the Royal Society of Tropical Medicine and Hygiene*, *72*(1), 6–15.

BBC Monitoring and UGC Newsgathering. (2020). *BBC Monitoring: China coronavirus: misinformation spreads online*, available at https:// www.bbc.com/news/blogs-trending-51271037

Centers for Disease Control and Prevention. (2012). *Lesson 1: Introduction to Epidemiology*, available at https://www.cdc.gov/csels/ dsepd/ss1978/lesson1/section8.html

Charlet, K. (2018). *The New Killer Pathogens: Countering the Coming Bioweapons Threat*, available at https://www.foreignaffairs.com/world/new-killer-pathogens

Chen, Y., & Li, L. (2020). Sars-cov-2: virus dynamics and host response. *The Lancet Infectious Diseases*, *20*(5), 515-516.

Christian, M. D. (2013). Biowarfare and bioterrorism. *Critical care clinics*, *29*(3), 717–756.

Clarke, G. (2020). *COVID-19 threatening global peace and security, UN chief warns.* UN News, available at https://news.un.org/en/ story/2020/04/1061502.

Dembek, Z. F., Kortepeter, M. G., & Pavlin, J. A. (2007). Discernment between deliberate and natural infectious disease outbreaks. *Epidemiology & Infection*, *135*(3), 353–371.

Garrett, L. (2021). The Forgotten Biological Terror of 9/11. *Foreign Policy*, available at https:// foreignpolicy.com/2021/09/10/ the-forgotten-biological-terror-of-9-11/

Gulis, G., & Fujino, Y. (2015). Epidemiology, population health, and health impact assessment. *Journal of epidemiology*, *25*(3), 179–180.

Harrington, D. M., & Hadjiconstantinou, M. (2022). Changes in commuting behaviours in response to the covid-19 pandemic in the uk. *Journal of transport & health*, *24*, 101313.

Heads of State and Government. (2002). Press Release (2002)127: Prague Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague. *NATO*, available at https://www.nato.int/docu/0211prague/ speeches-e.pdf

Iftimie, I. A. (2020). The implications of covid-19 for nato's counter-bioterrorism. *COVID-19: NATO in the Age of Pandemics*, 51–59.

Islington Council (2023). *The role of local authorities*, available at https://www. islington.gov.uk/about-the-council/ who-we-are/how-the-council-works/the-role-of-a-local authority#:~:text=They%20represent%20their%20local%20communities,priorities%20and%20provide%20community%20leadership.

Jenkins, B. (2017). The global health security agenda and the role of the world organisation for animal health. *Revue Scientifique et Technique (International Office of Epizootics)*, *36*(2), 639–645.

Kiss, I. Z., Berthouze, L., Taylor, T. J., & Simon, P. L. (2012). Modelling approaches for simple dynamic networks and applications to disease transmission models. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *468*(2141), 1332–1355.

Koblentz, G. D., Lentzos, F., Houser, R., Ameneiros, M., Earnhardt, B., Rodgers, J., & Wingo, H. (2023). *GlobalBioLabsReport2023*, available at https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/ 1678955285754/KCL0680_BioLabs+Report_Digital.pdf

Koopman, J. (2004). Modeling infection transmission. *Annu. Rev. Public Health*, *25*, 303–326.

Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). Covid-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs*, 1–22.

Lyon, R. F. (2021). The covid-19 response has uncovered and increased our vulnerability to biological warfare. *Military medicine*, *186*(7-8), 193–196.

Marchment, Z., & Gill, P. (2022). Spatial decision making of terrorist target selection: Introducing the track framework. *Studies in Conflict & Terrorism*, *45*(10), 862–880.

McLoughlin, D. (1985). A framework for integrated emergency management. *Public administration review*, *45*, 165–172.

North Atlantic Treaty Organization. (2022). *Weapons of mass destruction*, available at https://www.nato.int/cps/en/natohq/topics_50325.htm

Perry, R. W., & Mankin, L. D. (2005). Preparing for the unthinkable: Managers, terrorism and the HRM function. *Public Personnel Management*, *34*(2), 175–193.

Radosavljevic, V., & Belojevic, G. (2012). Unusual epidemic events: a new method of early orientation and differentiation between natural and deliberate epidemics. *Public Health*, *126*(1), 77–81.

Remarks by the President in Photo Opportunity with Members of Congress, The Cabinet Room. (2001). President Says Terrorists Won't Change American Way of Life. *Office of the Press Secretary*, available at https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/text/20011023-33.html

Riedel, S. (2004). Biological warfare and bioterrorism: a historical review. *Health Affairs*, *17*(4), 400–6.

Riley, S. (2007). Large-scale spatial-transmission models of infectious disease. *Science*, *316*(5829), 1298-1301.

Rothman, K. J. (1976). Causes. *American journal of epidemiology*, *104*(6), 587–592.

Sloan, S. (2002). Meeting the terrorist threat: The localization of counter terrorism intelligence. *Police Practice and Research*, *3*(4), 337–345.

Snyder, G. H. (2015). *Deterrence and defense* (Vol. 2168). Princeton University Press.

Thompson, K. M. (2016). Evolution and use of dynamic transmission models for measles and rubella risk and policy analysis. *Risk Analysis*, *36*(7), 1383–1403.

United Nations. (1972). *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction,* , available at https://legal.un.org/avl/ha/cpdpsbbtwd/cpdpsbbtwd.html

Vidino, L., & Hughes, S. (2015). Countering violent extremism in America. *The George Washington University Center for Cyber Homeland.*

Defence Against Terrorism Review DATR Magazine

E-DATR, 2023; 18 : 27-44
Electronic Online ISSN 1307 - 9190
https://dergipark.org.tr/tr/pub/datr

The Nexus Between Climate Change and Terrorism and its Ramificiations in the Global South and the Global North

Zeynep Sütalan[1]

Abstract

Climate change's interaction and convergence with other risks and pressures can exacerbate conflicts and increase instability. The global community has agreed upon defining climate change as a 'threat multiplier' as to reveal its challenging impacts. This article addresses the impact of climate change on terrorism as a 'threat multiplier', especially how it lays a fertile ground for terrorist recruitment and radicalization. In this regard, how the root causes of terrorism intersect with climate change is analyzed together with how climate change impacts terrorism. The article reflects on the importance of contextuality about the impact of climate change on terrorism and argues that the impact of climate change in the Global South differs from the Global North, and understanding these differences is important for better threat assessments.

Keywords: Climate Change, Terrorism, Terrorist Recruitment, Global South, Global North

[1] PhD, International Relations, Free-lance Researcher.

1. Introduction

Climate change[2] has begun to garner attention as a 'threat multiplier' in security especially in the last decade. For instance, NATO, a political military alliance, which is based on the principle of collective defense and founded upon the conventional military thinking of the Cold War era, accepted climate change as "one of the defining challenges of our time"[3]. Recognizing its potential impact on the security of the Alliance, NATO states that climate change is both a crisis and a threat multiplier.[4] Climate change is considered a threat multiplier as it causes extreme weather conditions and thus increases the likelihood of environmental disasters like floods and forest fires, it leads to a rise in sea levels, brings about the depletion of natural resources, causes drought and land degradation leading to food scarcity, any of which can ultimately lead not only to humanitarian disasters including migration, but can also lead to increased tensions, conflict and ultimately violence within and between societies. Furthermore, climate change is not a problem only for some countries in the world. Regions like Africa, Southeast Asia, and the Caribbean might seem to witness the impact of climate change in a more drastic way compared to the other parts of the worlds, but in fact no country is immune to the effects of climate change. However, as indicated in the Global Climate Risk Index 2021, the developing world is affected more by the impacts of climate change, because they are more vulnerable to damaging impacts of hazards due to their lower capacities of coping.[5]

The recent study by Jerimiah O. Asaka underline that of 112 documents published between 2000 and 2020 about climate change and/or security and/or terrorism, 53 documents explore the climate-security nexus whereas only 18 documents explore the interaction between climate change and terrorism.[6] Thus,

---

2 United Nations Framework Convention on Climate Change (UNFCCC) defines 'climate change' as: "a change of climate which is attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability observed over comparable time periods." See Article 1 of the UNFCCC, available at https://unfccc.int/sites/default/files/convention_text_with_annexes_english_for_posting.pdf (accessed on 1 April 2023).

3 *NATO Climate Change and Security Action Plan*, available at https://www.nato.int/cps/en/natohq/official_texts_185174.htm (accessed on 1 April 2023).

4 NATO 2022 Strategic Concept, available at https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (accessed on 7 December 2023).

5 *Global Climate Risk Index 2021*, available at https://reliefweb.int/report/world/global-climate-risk-index-2021 (accessed 01 April 2023)

6 Jeremiah O. Asaka, "Climate Change-Terrorism Nexus? A Preliminary Review/analysis of the Literature", *Perspectives on Terrorism*, (Vol. 15, No.1, February 2021), p. 86.

the impact of climate change on security has been more recognized than the relative interplay between climate security and terrorism. Despite the scarcity of research and the little attention to the link(s) between climate change and terrorism, the mainstream approach to the relationship between climate change and terrorism underscores that there is not a direct relationship between terrorism and climate change, and thus climate change is a instead 'threat multiplier'.[7] This means that climate change intersects with and has the potential to aggravate other security threats. As stated by the United Nations (UN) Secretary-General António Guterres: "Climate change is not the source of all ills, but it has a multiplier effect and is an aggravating factor for instability, conflict and terrorism."[8] According to Stephanie Mavrakou et.al., the term 'threat multiplier' is first used in a report titled "National Security and The Threat of Climate Change"[9] published in 2007 by CNA Corporation.[10] Afterwards, the term started being used first by the US Department of Defense and the UN to denote the impact of climate change on security.[11]

Although there is not a direct correlation between climate change and terrorism, climate change serves as a 'threat multiplier' in terrorism. Therefore, this article explores the impact of climate change on terrorism, especially how it lays a fertile ground for terrorist recruitment and radicalization. With this goal in mind, it investigates how the root causes of terrorism intersect with climate change and how climate change contributes to the push and pull factors of terrorist recruitment. The article reflects on the salience of contextuality regarding the impact of climate change on terrorism and argues that the impact of climate change in the developing world (referred as Global South) differs from the developed world (referred as Global

---

7 Ibid, pp.87-90; Stephanie Mavrakou, Emelie Chace-Donahue, Robin Oluanaigh and Meghan Conroy, "The Climate Change- Terrorism Nexus: A Critical Literature Review", *Terrorism and Political Violence*, (Vol. 34, no.5, 2022), p.899; *NATO Climate Change and Security Action Plan* and referred as "risk-multiplier in UNDP, *The Climate Security Nexus and the Prevention of Violent Extremism* (New York: UNDP, 2020). https://www.undp.org/sites/g/files/zskgke326/files/publications/UNDP-Climate-Security-Nexus-and-Prevention-of-violent-extremism.pdf

8 "Climate Change 'a Multiplier Effect', Aggravating Instability, Conflict, Terrorism, Secretary-General Warns Security Council", UN Meetings Coverage and Press Releases, 9 December 2021, available at https://press.un.org/en/2021/sgsm21074.doc.htm (accessed on 8 June 2023).

9 It is stated in the report as: "Climate change acts as a threat multiplier for instability in some of the most volatile regions of the world". See *National Security and The Threat of Climate Change*, CNA Corporation, 2007,6, available at https://www.cna.org/archive/CNA_Files/pdf/national%20security%20and%20the%20threat%20of%20climate%20change.pdf (accessed on 8 June 2023).

10 Mavrakou et.al., "The Climate Change- Terrorism Nexus", p. 908.

11 Ibid.

North). There are different dynamics at play in these two different regions, although these are not totally independent from each other in the highly interconnected globalized world.

2. What Causes Terrorism and Where Does Climate Change Fit in?

Terrorism is a political phenomenon, but there is no universally agreed definition for terrorism, because different states, scholars[12] and international organizations[13] have different definitions of terrorism. One of the main reasons for the absence of universal definition is the political nature of terrorism, as widely reflected on the famous aphorism of 'one man's terrorist is another man's freedom fighter'. Even though the lack of a universally-agreed definition of terrorism is still seen as one of the primary factors that hampers international cooperation, the international community has moved on with different legal instruments[14] to promote international cooperation in the fight against terrorism.

Today what is generally meant by terrorism is a non-state actor using unlawful violent acts to intimidate people to achieve political objectives. Additionally, a relatively new term has become widely used, sometimes interchangeably with terrorism: 'violent extremism'.[15] In fact, violent extremism is a broader term compared to terrorism.[16] However, violent extremism also lacks a universally agreed definition, and "the term 'extremism' has no basis in binding international

---

12 The first renown academic endeavor regarding the definition of terrorism dates back to the early 1980s. Alex P. Schmid catalogued 109 different definitions of terrorism used between the years 1936-1980, the majority of which were scholarly definitions. He identified 22 definitional elements. Among them the most referred ones were "violence", "political", "fear" and "threat". See Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, And Literature*, (New Brunswick: Transaction Books, 1988), p. 5

13 NATO defines terrorism in NATO Glossary of Terms and Definitions AAP-6 as: "The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives."

14 An example for such legal instruments can be 1977 European Convention on the Suppression of Terrorism. Additionally, United Nations Security Council (UNSC) have adopted several resolutions concerning terrorism and counterterrorism starting from UNSC Resolution 1269 (1999). For the list of UNSC terrorism-related resolutions, see "Security Council Resolutions", available at https://www.un.org/securitycouncil/ctc/content/security-council-resolutions (accessed on 10 June 2023).

15 William Stephens, Stijn Sieckelinck and Hans Boutellier, "Preventing Violent Extremism: A Review of Literature", *Studies in Conflict and Terrorism*, (Vol.44, No.4, 2021), pp.346-361.

16 Violent Extremism can also include extreme right-wing groups which may not always be considered as terrorists. See "A New Approach? Deradicalization programs and Counterterrorism", Meeting Note, June 2010, available at https://www.ipinst.org/wp-content/uploads/publications/a_new_approach_epub.pdf (accessed on 10 June 2023).

legal standards"[17]. Additionally, about the definition of terrorism and its relation to violent extremism, Alex P. Schmid mentions:

> When this author googled (*sic*) 'definition of terrorism' back in 2014, he got 48 million hits; in 2019 there were 136 million and, by mid-2022, there were 238 million hits. While many people wish to know more about this type of politically motivated crime, there are also those who seem to have given up and wonder: "is terrorism worth defining?" Yet others no longer talk about 'terrorism' and prefer the term 'violent extremism'. However, such a shift away from 'terrorism' to defining 'extremism' does not solve much. Unlike 'terrorism' (or 'radicalism'), 'extremism' has not been a self-description of militant political actors. Extremism as a label was first used more widely only in the first half of the 20th century, referring mainly to communist and fascist movements and regimes, and, secondarily, to some excesses of hyper-nationalism.[18]

Terrorism is a complex phenomenon, the roots of which may originate from different causes at different levels ranging from structural to individual. Tore Bjørgo offers a classification of causes of terrorism according to the level of causation as: "Structural causes", "facilitator (accelerator) causes", "motivational causes" and "triggering causes".[19] "Structural causes" stem from macro level and can be found in the milieu, be it the characteristics of the international system, or the political, cultural, social and economic structures of the states and societies. Examples include: "demographic imbalances, globalization, rapid modernization, transitional societies, increasing individualism with rootlessness and atomization, relative deprivation, class structure, etc."[20] "Facilitator causes" are not the main causes of terrorism, but they enable terrorism and help terrorism attract widespread attention. The increase in the speed of the means of transportation and communication, together with their relatively low costs, the modern news

[17] "About protecting human rights while countering terrorism and violent extremism", available at https://www.ohchr.org/en/terrorism/about-protecting-human-rights-while-countering-terrorism-and-preventing-violent-extremism (accessed on 10 June 2023).

[18] Alex P. Scmid, "Defining Terrorism", ICCT Report, March 2023, available at https://www.icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf (accessed on 05 June 2023)

[19] Tore Bjørgo, "Introduction", Tore Bjørgo (ed.), *The Root Causes of Terrorism: Myths, Reality and Ways Forward*, (New York, Oxon: Routledge, 2005), pp.3-4.

[20] Ibid, 3.

media, developments in the weapons technology, state sponsoring, weak state control of territory and weak governance of precious minerals like oil, gold and diamonds can be counted among facilitator causes of terrorism.[21] "Motivational causes" is about why people engage in terrorism, and thus about grievances. These may include psychological to ideological factors as motivations or what may be considered as 'radicalization'. Again lacking a uniform definition, radicalization can be defined as "the framework of choice for analyzing what brings individuals and groups to terrorism"[22]. Being considered as a process, radicalization is conceptualized or modelled as phases or steps[23] with the inherent weakness that the process can stop anywhere and may not lead to the violent action.[24] In addition to examining an individual's engagement in terrorism through radicalization, another approach may be through studying personal motives. Mia Bloom offers the classification of women's motives for joining terrorist organizations as Four 'R's -revenge, redemption, relationships, and respect- and then expanded it to five 'R's with the inclusion of rape.[25] In fact, these categories can also apply to the case of men's involvement in terrorism, albeit in different ways. On the other hand, the problem with studying individuals' radicalization process is that there are too many variables that can be counted in the radicalization process. This means that "we do not really know what radicalizes people. Certain factors might lead to the radicalization of an individual whereas the same factors might not lead to the radicalization of another individual"[26]. Therefore, the radicalization process differs from one individual to another. There are many other factors that interplay to define an individual's vulnerability to a terrorist mobilization and propaganda. Moreover, as Eviane Leidig claims for the case of far-right movements, it can

21 Ibid and Zeynep Sutalan, "The Causes of Terrorism", COE-DAT (ed.), *Organizational and Psychological Aspects of Terrorism*, (Amsterdam: IOS Press, 2008), p.5.

22 European Parliament, "Preventing Radicalisation in the European Union: How EU policy has evolved", (Brussels: European Union, 2022), available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/739213/EPRS_IDA(2022)739213_EN.pdf (accessed 10 June 2023)

23 For the most renown models, see Randy Borum, "Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research", *Journal of Strategic Security*, (Vol 4 , no. 4, 2011), pp. 37-62.; F. M. Moghaddam, "The Staircase to Terrorism: A Psychological Exploration", *The American Psychologist*, (Vol. 60, No.2, 2005), pp.161-169, and C. McCauley and S. Moskalenko, "Mechanisms of political radicalization: pathways toward terrorism", *Terrorism and Political Violence*, (Vol. 20, Issue 3, 2008), pp.415-433.

24 European Parliament, "Preventing Radicalization".

25 Mia Bloom, "Bombshells: Women and Terror", *Gender Issues,* (Vol. 28, no.1, 2011), pp.1-21.

26 COE-DAT, "Women in Terrorism and Counterterrorism", *Workshop Report*, (COE-DAT: Ankara, 2019), p. 48.

also apply to different types of terrorism: "recruitment and radicalization should be understood interchangeably" [27] , because it is not definite which comes first. Sometimes an individual is recruited to a terrorist group and then radicalized, or sometimes first radicalized and then recruited and radicalization and recruitment appear as interlinked process and occur at the same time.[28] When it comes to the final category of Bjørgo as "triggering causes"[29], these are "the immediate circumstances or events that provoke people to resort to engaging in terrorism. Normally, these events or circumstances may not lead to terrorism. However, given the existing conflicts and tensions, these events play a triggering role and set off terrorist actions. Triggering causes may be a war, the rise of a leader or revenge for a killing"[30].

In order to understand 'why terrorism occurs', we need to find out 'where and under what circumstances terrorism emerges' and 'why people become terrorists'. Tore Bjørgo and Andrew Silke argue: "The discussion on whether the emergence of terrorism can be understood mainly as an outcome of root causes or as an outcome of individual processes of radicalisation and choices relates to a more general debate in the social sciences over what is more important in shaping human behavior – structure or agency."[31] From this point onwards, this article suggests that both the macro-level structural dynamics and individual-level motivational dynamics are reinforcing each other in the emergence of terrorism, and this necessitates examining different levels.

How climate change intersects with 'root causes of terrorism' requires a closer examination of the macro-level causes of terrorism, which are identified with "systemic conditions at the level of society, state, international relations, and/or trans-national developments"[32]. These causes include intra-state and inter-state conflicts, invasions, occupations, bad governance, rapid modernization, class structures and relative deprivation, unemployment and poverty, lack of

[27] Eviane Leidig, *"We are worth fighting for:" Women in Far-Right Extremism, (*ICCT, 26 Oct 2021), available at https://www.icct.nl/publication/we-are-worth-fighting-women-far-right-extremism (accessed on 10 June 2023).

[28] Ibid.

[29] Bjørgo, "Introduction", p. 4.

[30] Sutalan, "The Causes of Terrorism", p. 9.

[31] Tore Bjørgo and Andrew Silke, "Root Causes of Terrorism," in *Routledge Handbook of Terrorism and Counterterrorism*, edited by Andrew Silke (Oxon, UK: Routledge, 2018), p.63.

[32] Andrew Silke and John Morrison, "Gathering Storm: An Introduction to the Special Issue on Climate Change and Terrorism", *Terrorism and Political Violence*, Vol.34, No.5, 2022, p. 883.

democracy and political representation. These causes may not necessarily lead to terrorism, but may create a fertile ground for tension and conflict where terrorism can thrive. Climate change together with population growth, migration and social polarization are counted among the emerging macro-level causes of terrorism.[33] By affecting both the quality and quantity of natural resources adversely, climate change exacerbates social tensions. By increasing food and water insecurity, it can threaten people's livelihoods. Besides, limited or no access to natural resources or ceasing sources of livelihood including farming can lead to rural to urban migration, potentially fueling social tensions. When these potential risks are combined with governments' incapacity to timely and adequately respond to the impacts of climate change and meet the needs of its people, it can increase popular discontent enabling terrorists to extend their reach.

3. How does the Climate Change Impact Terrorism? Differences of Global North and Global South

The relationship between climate change and terrorism is formed in a different way in the Global South and Global North, bringing in the salience of contextuality in understanding terrorism. Despite the fact that these two contexts tell different stories, they are not totally independent from each other. In the Global South, climate change exacerbates the socio-economic conditions and paves ground for terrorist recruitment and radicalization. In the Global North, ecofascism (a right-wing ideology which blames overpopulation), immigration, over-industrialization for environmental degradation, turns out to be a motivational factor for some terrorist attacks such as in the cases of Christchurch, New Zealand mosques attacks in 2019 and El Paso mass shootings in the US the same year. Climate change-induced dire environmental conditions generally lead to migration within a state, and generally from rural to urban.[34] However, there are also cases where people are forced to leave their homelands. Sometimes this movement of migration is from Global South to Global North. In the Global North, climate-induced migration from the Global South may encourage violent extremist ideologies as well as playing into the hands of the far-right violent extremists and right-wing terrorism which rely

[33] Ibid, p.863.

[34] For the analysis of how climate-change induced rural-urban migration might increase the risk of terrorism, see John Schon and Stephen Nemeth, "Moving into Terrorism: How Climate-Induced Rural-Urban Migration May Increase the Risk of Terrorism", *Political Violence and Terrorism*, (Vol. 34, No.5, 2022), pp.926-938.

on anti-immigration rhetoric and narratives.

Additionally, eco-terrorism or environmental extremism is also a concern especially for the governments in the Global North. However, Silke and Morrison argue that eco-terrorism and environmental extremism have not been a substantial threat for the last four decades.[35] Referring to the records from Global Terrorism Database (GTD), Silke and Morrison underline that it is only the 0.1 % of 200,000 terrorist incidents since 1970 that were executed by "a group or individual motivated by an environmentally related ideology"[36].

3.1. Global South: The Impact of Climate Change on Terrorism

The developing world is susceptible to conflict and "the adverse effects of the climate change"[37]. Since most of the population in these regions rely on agriculture and pastoralism for living, they are heavily affected by the changes in the climate. Additionally, the states in these regions are not able to maintain law and order and provide basic services to their citizens. Then the susceptibility of livelihoods combined with the low capacity of states creates vulnerabilities to conflict.[38] As mentioned by the UN Secretary-General António Guterres, "Of the 15 countries most exposed to climate risks, eight host a United Nations peacekeeping or special political mission. Climate impacts compound conflicts and exacerbate fragility."[39] Weak or fragile states already suffering from poorly-functioning institutions, lack of capacity to provide basic social services, and lack of order, are worn down by the adverse effects of the climate change. This increases existing grievances or creates new ones in the given society, decreasing their trust to their government. People who have lost their livelihoods or homes because of climate change-induced extreme weather conditions like drought, floods, wildfires, etc., and do not have any prospects for regular income and protection by the government become easy prey for the terrorist organizations.

---

35 Silke and Morrison, "Gathering storm", 889-91.

36 Ibid, 889.

37 UNFCC defines the adverse effects of climate change as: "changes in the physical environment or biota resulting from climate change which have significant deleterious effects on the composition, resilience or productivity of natural and managed ecosystems or on the operation of socio-economic systems or on human health and welfare." See Article 1 of the UNFCCC.

38 See Oseloka H. Obaze et al.," Climate Change as a Security Threat in Nigeria and The Sahel", *Friedrich-Ebert -Stiftung Nigeria Policy Brief*, June 2022, available at https://library.fes.de/pdf-files/bueros/nigeria/19957.pdf (accessed 10 November 2023).

39 "Climate Change 'a Multiplier Effect'"

Terrorist organizations exploit the vulnerabilities exacerbated by the impacts of the climate change and manipulate resource scarcity for terrorist recruitment and radicalization.[40] In Somalia, Al Shabaab has appeared as the alternative service provider at times of frequent droughts, resultant internal displacement and chronic food scarcity and insecurity. In this way, the terrorist organization not only strengthened its legitimacy, but also increased its recruitment.[41] Additionally, Al Shabaab uses criminal activities like livestock trafficking, charcoal and sugar smuggling, piracy and petty crime apart from human, arms and drug trafficking not only to finance the terrorist organization, but also as a means of recruitment.[42] Katharine Petrich in her field research about Al Shabaab underlines that many young men start as petty criminals before they become terrorists, no doubt, but a terrorist organization's recruitment strategy is not limited to that. Then she discusses about a consistent pattern of recruitment as "young adults were contacted, either in person or over social media, with promises of employment – often in the hospitality industry in Somalia, Northern Kenya, or the Gulf States – and were asked to travel to meet their employment sponsors. When they arrived, Al Shabaab militants took them to recruitment camps for training (in the case of men) or sexual/domestic slavery (for women)."[43] Similarly, Boko Haram as a terrorist organization operating in Nigeria, has not only been able to recruit members from Nigeria, but also from Cameron, Chad, Niger, Mali and Libya. Among many strategies Boko Haram utilizes for recruitment is the "promise of better welfare and improved economic conditions"[44]. Research has displayed that most of the people joining Boko Haram mentioned the lack of economic opportunities and unemployment as their reasons for getting involved in the organization.[45] Boko Haram has been able to capitalize on the incapacity of the government to provide its people with economic welfare.

---

40 See Catherine Wong, "Gender in Climate Security Perspective of PVE" in COE-DAT, "Gender in Terrorism and Counterterrorism: Unravelling Masculinities, The Impact of Climate Change and Cyber Security", *Workshop Report*, (COE-DAT: Ankara, 2023), pp.38-41.

41 "The climate security nexus and the prevention of violent extremism: Working at the intersection of major development challenges", *UNDP Policy Brief*, (UNDP, 2020), available at https://www.undp.org/publications/undp-climate-security-nexus-and-prevention-violent-extremism (accessed on 8 October 2023).

42 Katharine Petrich, "Cows, Charcoal and Cocaine: Al Shabaab's Criminal Activities in the Horn of Africa", Studies in Conflict and Terrorism, (2019), pp.1-22. DOI:10.1080/1057610X.2019.1678873

43 Ibid, pp.9-10.

44 Kangdim Dingji Maza, Umut Koldas, and Sait Aksit, "Challenges of Countering Terrorist Recruitment in the Lake Chad Region: The Case of Boko Haram", *Religions*, (Vol.11, no. 2, 2020), p. 96. https://doi.org/10.3390/rel11020096

45 Ibid.

Therefore, livelihood insecurity turns out to be one of the main drivers for people to join Boko Haram and for the terrorist organization is a source of manipulation where root causes of terrorism intersects with climate change.[46]

Terrorist organizations can deprive populations of food, water and other supplies by blockading towns for forcing them to submission. "Terrorist organizations have not just leveraged climate change induced resource shortages, they have also created new shortages to establish community dependency, garner influence, and recruit new members."[47] Al Shabaab demands taxes in the areas they control and at hard times of climate change-induced dire conditions like droughts, people may not have any choice but to leave their land or join the terrorist organization. Daesh in Iraq and Syria used its control over vital water resources and infrastructure as a tool of subjugation and creating community dependency. Daesh exploited water as a weapon of blackmail to force local populations to comply with its demands, and people had little choice other than to abide by the orders of the Daesh, because water has always been a scarce resource in the region and conditions worsened after the droughts in the first decade of the 2000s.[48]

Another critical issue regarding the nexus between climate change and terrorism in the Global South is the gender aspect which exacerbates the already existing inequalities in the societies to the disadvantage of women and girls. Women's working load increases and they often become sole providers and caregivers for the household, in many cases making them *de facto* heads of the household since their husbands either died, left because of conflict or joined the terrorist groups. Climate change also increases vulnerabilities of women risking their health and security when they had to travel long distances for collecting water and firewood and making them targets of sexual and gender based violence by the terrorists.[49] They can either be kidnapped as sex slaves or forced into marriage. In areas highly affected by terrorism and climate change induced dire conditions, women

---

46 For a detailed analysis of the climate change, and conflict in Lake Chad Basin, see Chitra Nagarajan, Benjamin Pohl, Lukas Rüttinger, Florence Sylvestre, Janani Vivekananda, Martin Wall and Susanne Wolfmaier, *Climate-Fragility Profile: Lake Chad Basin*, (Berlin: adelphi, 2018).

47 John P. Sullivan and Keely Townsend, "Climate Migration: Adding Fuel to Ethnocentric Fire", *Terrorism and Political Violence* (Vol. 34, No.5, 2022), p. 920.

48 "Water and Violence: Crisis of Survival in the Middle East", (Strategic Foresight Group, Mumbai, 2014), available at https://www.files.ethz.ch/isn/188318/63948150123-web.pdf (accessed on 8 October 2023).

49 Nazanine Moshiri, "Gender, Climate Change and Terrorism in Africa: Gendered Impact of Climate-Terrorism Link" in COE-DAT, "Gender in Terrorism and Counterterrorism", *Workshop Report*, 2023, pp.42-45.

form the majority of IDP (Internally Displaced Person) camps whereas men join the terrorists or, conversely, fight against the terrorists and/or stay to protect their livestock, fields, and houses. Once again displaced women and girls are confronted by high risk of violence and sexual abuse, including sexual harassment and rape. Terrorist organizations also restrict the movement of people, goods and resources and this have serious consequences for women. Women, especially the pregnant and breastfeeding, face malnutrition as well as no access to essential services including healthcare. Last, but not the least, terrorist organizations can also force women to join them to perpetrate suicide attack or coerce them to smuggle goods by exploiting gender biases that women can evade security checks and raise less suspicion.[50]

3.2. Global North: Ecofascism and Terrorism

The extreme right is globally on the rise.[51] It is not just a problem of the Global North[52], and it is a threat to law and order and democracy in the Global South, too. However, although right-wing ideology and groups have always existed in Europe, the large increase in the right-wing in the 2010s is due to the growth in immigration from predominantly underdeveloped and/or developing countries, the increased mobility of individuals within the European Union and normalization of far-right ideas in political populist discourse.[53] In the context of rising far-right in the Global North, ecofascism[54] has appeared as a motivational factor for potential future attacks in the Christchurch (New Zealand) and El Paso (Texas, US) terrorist attacks, because in their the pre-attack manifestos, the terrorist perpetrators of these attacks identified themselves as ecofascists. Brenton Tarrant, the Christchurch terrorist, who entered first into the Al Noor Mosque and then the Linwood Islamic

50 For more see, COE-DAT, "Gender in Terrorism and Counterterrorism: Unravelling Masculinities, The Impact of Climate Change and Cyber Security", *Workshop Report*, (COE-DAT: Ankara, 2023).

51 Heather Ashby, "Far Right Extremism is a Global Problem", Foreign Policy (15 January 2021), available at https://foreignpolicy.com/2021/01/15/far-right-extremism-global-problem-worldwide-solutions/

52 Tanya Mehra and Naureen Chowdhury Fink, "Violent Far-Right Movements Aren't Just a 'Western Problem'", Ideas, 15 March 2023, available at https://www.defenseone.com/ideas/2023/03/violent-far-right-movements-arent-just-western-problem/384003/

53 Ashby, "Far-right Extremism".

54 Farrell-Molloy and Macklin underlines that ecofascism is a contested concept and there are other proposals by different scholars like 'neo-ecofascism', 'right-wing ecologism' and 'far-right ecologism'. See Joshua Farrell-Molloy and Graham Macklin, "Ted Kaczynski, Anti-Technology Radicalism and Eco-Fascism", *ICCT Perspective*, 15 June 2022, https://www.icct.nl/publication/ted-kaczynski-anti-technology-radicalism-and-eco-fascism

Center during the Friday Prayers in Christchurch in New Zealand killing 51 people proclaimed himself as ethnonationalist and ecofascist who is fighting against the 'invaders' (immigrants).[55] Later the same year, Patrick Wood Crusius shot death 23 people at a Walmart store in the El Paso attack claiming support to the Christchurch terrorist Tarrant and referring to grievances from environmental degradation and demographical changes by 'Hispanic invasion'. Both terrorist perpetrators posted manifestos online complaining about immigrants- Tarrant mainly targeting the Muslim immigrants whereas Crusius targeted Hispanics. "Both manifestos also espoused environmental protection as a component of their motivation, seeking to prevent the overexploitation of resources by eliminating undesirable outgroups, and thus, allowing ingroups (White Christians) to achieve ecological sustainability while maintaining desired lifestyles."[56] After these two terrorist attacks, discussions about ecofascism as an ideology together with climate change and environmental degradation as motivational factors in the right-wing terrorism gained momentum.

Ecofascists[57] are generally viewed within the broader extreme right ideology favoring a community of people, believed to be chosen to live on a particular land. The idea is that this community of people constitute an ethnicity or race which has a mystical connection to the land they live. Therefore, there is a natural order dividing people as different ethnicities or races belonging to different lands. This ecological harmony is disrupted by certain processes such as industrialization, modernization, urbanization, immigration, overpopulation (which is disproportionate in ethnicity or race). People who are not the member of that ethnicity or race and thus do not share the same connection with the land should be expelled or exterminated since they are disturbing the social and ecological harmony. Such approach is obviously anti-human sharing the similar 'Blood and Soil' idea of the Nazi ideology dating back to the early 20th century. Hence they believe in the salvation of the community can only be possible through getting rid of disrupting and polluting elements and also in reconnection of human beings with nature in line with their

---

55 Brenton Tarrant, *The Great Replacement*, available at https://commons.wikimannia.org/images/Tarrant_Brenton_-_The_Great_Replacement.pdf (accessed on 08 October 2023)

56 Sullivan and Townsend, "Climate Migration", p. 920.

57 For detailed analysis and discussions about Ecofascism, see Graham Macklin, "The Extreme Right, Climate Change and Terrorism", *Terrorism and Political Violence*, (Vol. 34, No.5, 2022), pp.979-996, and Brian Hughes, Dave Jones & Amarnath Amarasingam, "Ecofascism: An Examination of the Far-Right/Ecology Nexus in Online Space", *Terrorism and Political Violence*, (Vol. 34, No.5, 2022), pp.997-1023.

connections to the land. In this vein, Kristy Campion defines ecofascism as "a reactionary and revolutionary ideology that champions the regeneration of an imagined community through a return to a romanticized, ethnopluralist vision of natural order"[58] underlining that ecofascism is more than combining fascism with ecologism.[59] Ecofascists connect the legitimate environmental concerns as a result of the climate change to supremacist ideologies and violence against minority groups.[60] According to Brian Hughes, what far-right extremists do is to recycle old hatreds rather than generating new ideas. Therefore, it is an illusionary justification of old patterns of racist violence to achieve the natural order free of any 'polluting' forces of the 'disastrous liberal project' and 'modernity'. [61] Not all scholars agree that ecofascism is a coherent ideology or a political movement, but it is highly likely that as the climate-change induced migration to the Global North from the Global South increases, ecofascist views and references will resonate more and more in extreme right environments.

Conclusion

Climate change is a reality of our time, and a global problem which has differing impacts in different parts of the world. Its interaction and convergence with other risks and pressures can exacerbate conflicts and increase instability. The global community agrees it is a 'threat multiplier' and used this concept as an effective way to grasp its challenging impacts. Climate change exacerbates and has the potential to aggravate present tensions and conflicts within and between societies since it increases the likelihood of environmental disasters like floods, droughts, wildfires leading to depletion of natural resources, land degradation, and thus water and food scarcity. Such pressures also have the potential to lead humanitarian disasters including migration. Where the relationship between climate change and terrorism is concerned, the mainstream approach to the nexus between climate change and terrorism denies a direct correlation between the two phenomena and views climate change as a 'threat multiplier' in the context of terrorism.

58 Kristy Campion, "Defining Ecofascism: Historical Foundations and Contemporary Interpretations in the Extreme Right", *Terrorism and Political Violence*, (Vol. 35, No.4, 2023), p. 927.

59 Ibid.

60 "Ecofascism –are far-right extremists the new environmentalists?", 29 July 2022, *ABC Podcast: Science Friction*, https://podtail.com/podcast/science-friction-abc-rn/ecofascism-are-far-right-extremists-the-new-envi-2/

61 Ibid.

Although climate change is a global problem, the Global South suffers exceptionally from the impacts of climate change, because the states in these regions lack enough capacity to deal with the adverse effects of the climate change. These societies are already exhibiting low levels of socio-economic development and educational opportunity, high levels of poverty, low levels of national integration, low social resilience, weak governance, volatile security environments or even ongoing conflicts. In such societies, people who do not have much choice for making their living become vulnerable to terrorist recruitment and radicalization. However, the impact of climate change is not the same in the Global North where different geographical characteristics, social, economic and political contexts lead to different impacts. Anxieties as a result of climate change are exploited by the right-wing terrorist groups or lone actors who define themselves as ecofascists to blame overpopulation, immigrants and over-industrialization for the contemporary environmental and ecological degradation, and propose racial violence as a way out of the climate change crisis. Against this backdrop, considering the importance of contextuality, more research examining the nexus between terrorism and climate change is required to feed policy-making to better tackle with these challenges.

Bibliography

"About protecting human rights while countering terrorism and violent extremism", available at https://www.ohchr.org/en/terrorism/about-protecting-human-rights-while-countering-terrorism-and-preventing-violent-extremism

"A New Approach? Deradicalization programs and Counterterrorism", Meeting Note, June 2010, available at https://www.ipinst.org/wp-content/uploads/publications/a_new_approach_epub.pdf.

Asaka, Jeremiah O. "Climate Change-Terrorism Nexus? A Preliminary Review/analysis of the Literature." *Perspectives on Terrorism*, (Vol. 15, No.1, February 2021), pp.81-92.

Ashby, **Heather.** "Far Right Extremism is a Global Problem". *Foreign Policy* , 15 January 2021. https://foreignpolicy.com/2021/01/15/far-right-extremism-global-problem-worldwide-solutions/

Bjørgo, Tore (ed.) *The Root Causes of Terrorism: Myths, Reality and Ways Forward*. (New York, Oxon: Routledge, 2005).

Bjørgo, Tore and Andrew Silke. "Root Causes of Terrorism." In *Routledge Handbook of Terrorism and Counterterrorism*, edited by Andrew Silke (Oxon, UK: Routledge, 2018), pp. 57-65.

Bloom, Mia. "Bombshells: Women and Terror". *Gender Issues,* (Vol. 28, no.1, 2011), pp.1-21.

Borum, Randy. "Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research". *Journal of Strategic Security*, (Vol. 4, no. 4, 2011), pp. 37-62.

Campion, Kristy. "Defining Ecofascism: Historical Foundations and Contemporary Interpretations in the Extreme Right". *Terrorism and Political Violence*, (Vol. 35, No.4, 2023), pp. 926-944.

"Climate Change 'a Multiplier Effect', Aggravating Instability, Conflict, Terrorism, Secretary-General Warns Security Council". UN Meetings Coverage and Press Releases, 9 December 2021.https://press.un.org/en/2021/sgsm21074.doc.htm

COE-DAT. "Women in Terrorism and Counterterrorism". *Workshop Report*, (COE-DAT: Ankara, 2019).

COE-DAT. "Gender in Terrorism and Counterterrorism: Unravelling Masculinities, The Impact of Climate Change and Cyber Security". *Workshop Report*, (COE-DAT: Ankara, 2023).

"Ecofascism –are far-right extremists the new environmentalists?", 29 July 2022, *ABC Podcast: Science Friction*, https://podtail.com/podcast/science-friction-abc-rn/ecofascism-are-far-right-extremists-the-new-envi-2/

European Parliament, "Preventing Radicalisation in the European Union: How EU policy has evolved", (Brussels: European Union, 2022), available at https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/739213/EPRS_IDA(2022)739213_EN.pdf

Farrell-Molloy Joshua and Graham Macklin. "Ted Kaczynski, Anti-Technology Radicalism and Eco-Fascism". *ICCT Perspective*, 15 June 2022. https://www.icct.nl/publication/ted-kaczynski-anti-technology-radicalism-and-eco-fascism

Global Climate Risk Index 2021. https://reliefweb.int/report/world/global-climate-risk-index-2021

Hughes, Brian, Dave Jones & Amarnath Amarasingam. "Ecofascism: An Examination of the Far-Right/Ecology Nexus in Online Space". *Terrorism and Political Violence*, (Vol. 34, No.5, 2022), pp.997-1023.

Leidig. Eviane. *"We are worth fighting for:" Women in Far-Right Extremism, (*ICCT, 26 Oct 2021), https://www.icct.nl/publication/we-are-worth-fighting-women-far-right-extremism.

Macklin, Graham. "The Extreme Right, Climate Change and Terrorism". *Terrorism and Political Violence*, (Vol. 34, No.5, 2022), pp.979-996.

Mavrakou, Stephanie, Emelie Chace-Donahue, Robin Oluanaigh and Meghan Conroy. "The Climate Change- Terrorism Nexus: A Critical Literature Review". *Terrorism and Political Violence*, (Vol. 34, no.5, 2022), pp.894-913.

Maza, Kangdim Dingji, Umut Koldas, and Sait Aksit. "Challenges of Countering Terrorist Recruitment in the Lake Chad Region: The Case of Boko Haram". *Religions*, (Vol.11, no. 2, 2020).https://doi.org/10.3390/rel11020096

McCauley, C. and S. Moskalenko. "Mechanisms of political radicalization: pathways toward terrorism". *Terrorism and Political Violence*, (Vol. 20, Issue 3, 2008), pp.415-433.

Mehra, Tanya and Naureen Chowdhury Fink. "Violent Far-Right Movements Aren't Just a 'Western Problem'". *Ideas*, 15 March 2023. https://www.defenseone.com/ideas/2023/03/violent-far-right-movements-arent-just-western-problem/384003/

Moghaddam, F. M. "The Staircase to Terrorism: A Psychological Exploration". *The American Psychologist*, (Vol. 60, No.2, 2005), pp.161-169.

Nazanine Moshiri, "Gender, Climate Change and Terrorism in Africa: Gendered Impact of Climate-Terrorism Link", in COE-DAT, "Gender in Terrorism and Counterterrorism: Unravelling Masculinities, The Impact of Climate Change and Cyber Security", *Workshop Report*, (COE-DAT: Ankara, 2023), pp.42-45.

Nagarajan, Chitra Benjamin Pohl, Lukas Rüttinger, Florence Sylvestre, Janani Vivekananda, Martin Wall and Susanne Wolfmaier. *Climate-Fragility Profile: Lake Chad Basin*, (Berlin: adelphi, 2018).

National Security and The Threat of Climate Change, CNA Corporation, 2007,6, available at https://www.cna.org/archive/CNA_Files/pdf/national%20security%20and%20the%20threat%20of%20climate%20change.pdf

NATO Climate Change and Security Action Plan, available at https://www.nato.int/cps/en/natohq/official_texts_185174.htm

NATO Standardization Office (NSO), *NATO Glossary of Terms and Definitions*: *AAP-06* Edition 2019.

Oseloka H. Obaze, Dr Chris M.A. Kwaja, Dr Freedom C. Onuoha, Dr Sunday Adejoh, Arigbabu Sulaimon, Chidiebere Ugwu. "Climate Change as a Security Threat in Nigeria and The Sahel". Friedrich-Ebert -Stiftung Nigeria Policy Brief. June 2022. https://library.fes.de/pdf-files/bueros/nigeria/19957.pdf

Petrich, Katharine. "Cows, Charcoal and Cocaine: Al Shabaab's Criminal Activities in the Horn of Africa". *Studies in Conflict and Terrorism*, (2019), pp.1-22. DOI:10.1080/1057610X.2019.1678873

Scmid, Alex P. “Defining Terrorism”. *ICCT Report*, March 2023. https://www.icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf

Schmid, Alex P. and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, And Literature*, (New Brunswick: Transaction Books, 1988).

Schon, John and Stephen Nemet. “Moving into Terrorism: How Climate-Induced Rural-Urban Migration May Increase the Risk of Terrorism”. *Political Violence and Terrorism*, (Vol. 34, No.5, 2022), pp.926-938.

Silke, Andrew and John Morrison. “Gathering Storm: An Introduction to the Special Issue on Climate Change and Terrorism”. *Terrorism and Political Violence*, (Vol.34, No.5, 2022), pp. 883- 893.

Stephens, William, Stijn Sieckelinck and Hans Boutellier, “Preventing Violent Extremism: A Review of Literature”, *Studies in Conflict and Terrorism*, (Vol.44, No.4, 2021), pp.346-361.

Sullivan John P. and Keely Townsend. “Climate Migration: Adding Fuel to Ethnocentric Fire”. *Terrorism and Political Violence* (Vol. 34, No.5, 2022), pp. 914-925.

Sutalan, Zeynep. “The Causes of Terrorism”. COE-DAT (ed.), *Organizational and Psychological Aspects of Terrorism*, (Amsterdam: IOS Press, 2008), pp.1-11.

Tarrant, Brenton. *The Great Replacement*. https://commons.wikimannia.org/images/Tarrant_Brenton_-_The_Great_Replacement.pdf

“The climate security nexus and the prevention of violent extremism: Working at the intersection of major development challenges”, *UNDP Policy Brief*, (UNDP, 2020). https://www.undp.org/publications/undp-climate-security-nexus-and-prevention-violent-extremism.

United Nations Framework Convention on Climate Change (UNFCCC). https://unfccc.int/sites/default/files/convention_text_with_annexes_english_for_posting.pdf

“Water and Violence: Crisis of Survival in the Middle East”, (Strategic Foresight Group, Mumbai, 2014).https://www.files.ethz.ch/isn/188318/63948150123-web.pdf.

Wong, Catherine. “Gender in Climate Security Perspective of PVE”. In COE-DAT, “Gender in Terrorism and Counterterrorism: Unravelling Masculinities, The Impact of Climate Change and Cyber Security”, *Workshop Report*, (COE-DAT: Ankara, 2023), pp.38-41.

Defence Against Terrorism
Review DATR Magazine

E-DATR, 2023; 18 : 45-66
Electronic Online ISSN 1307 - 9190
https://dergipark.org.tr/tr/pub/datr

Enhancing Cyber Defense and Resilience of Critical Infrastructures Against Terrorist Attacks[1]

Akın Aytekin
Mahir Dursun[2]

Abstract

Critical infrastructures such as power stations, heavy industries, transportation systems, electricity generation and telecommunication facilities are so vital to the countries that the impact or destruction of such systems could have an unprecedented effect on national security or safety. Industrial Control Systems (ICS) play an important role in critical infrastructures by providing process monitoring, remote and distributed control and automation. Due to the fact that critical infrastructures are mostly located in isolated places, Industrial Control Systems have recently become the targets of sophisticated cyberattacks.

In this paper, the structure of ICS is detailed and related security issues in terms of cybersecurity are explored. Because the main focus of the traditional ICS was system functions, network and system security were not considered during the design process. The development of information systems and communication technologies has forced governments and

---

1 This study has been conducted in the Research Assistantship Program (RAP) held by COE-DAT.

2 Akın AYTEKİN, aaytekin@tsk.tr (ORCID ID: 0000-0002-0783-7597) Information Security Engineering, Graduate School of Natural and Applied Sciences, Gazi University, Ankara, TÜRKİYE. Prof.Dr. Mahir DURSUN, mdursun@gazi.edu.tr (ORCID ID: 0000-0003-0649-2627) Department of Electrical and Electronic Engineering, Faculty of Engineering, Gazi University, Ankara, TÜRKİYE.

managers to adapt the design of ICS from isolated environments to interconnected ones and this makes ICS potentially more vulnerable than ever. In this article potential cyber attacks are reviewed in the light of identified vulnerabilities and previous incidents that have occurred over last decades. Threats and vulnerabilities are discussed and, in order to build more resilient Critical Infrastructures, some suggested standards, and recommendations are offered. Finally future research directions to enhance resilience in Critical Infrastructures are suggested.

Keywords: *Cybersecurity; Critical Infrastructure; Industrial Controls Systems; Resilience; SCADA.*

1. Introduction

Critical Infrastructures (CI) are those physical and cyber-based systems essential to the minimum operations of government and the economy[3]. Although there are a number of definitions and different classifications, most countries have identified their most valuable assets as CI and have strategic plans in order to protect them. Generally, CI can be classified as; the energy sector; water systems; transportation networks; nuclear facilities; commercial systems; emergency services; healthcare; government facilities; information technology; food and agriculture; financial services and so on.

Nations' critical infrastructures were initially designed as physically and logically separated systems and the most important issue to take into account was system functions. However, the unexpected speed of technological improvements forced CI to be more interconnected rather than isolated. Also, to fulfill industry requirements, most of the critical infrastructures have been connected to both enterprise and government networks in order to work with recent technologies such as big data analytics, the Internet of Things (IoT)[4] and artificial intelligence. To bear in mind, new technologies come with the new threats, especially from cybersecurity point of view.

Critical infrastructure can be vulnerable to various types of attacks, including physical and cyber attacks. Physical attacks could include acts of sabotage,

---

3 "The US Presidential Decision Directive/NSC-63", The White House, available at https://irp.fas.org/offdocs/pdd/pdd-63.htm (accessed 21 December 2022)

4 The Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks.

vandalism, or terrorism, while cyber attacks could include hacking, malware infections or denial-of-service attacks. But CI has often been designed to be much less secure against such advanced cyber attacks, so any compromise to CI may (and can) lead to significant physical danger to human lives. To protect against these types of incidents, CI typically implement a range of security measures, including perimeter security, access controls, and surveillance systems to detect and deter potential attackers.

To operate in isolated locations Industrial Control Systems (ICS), including supervisory control and data acquisition systems are used in most of critical infrastructures. Formally, the term of ICS covers numerous control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). ICS are combination of wireless and control components (e.g., electrical, mechanical, hydraulic, pneumatic) which achieve various industrial objectives (e.g., manufacturing, transportation of matter or energy).[5] Hence, ICS are the main target of cyber actors aiming to exploit and create damage.

Given the critical role of Industrial Control Systems in critical infrastructures, it is important to understand the security issues and vulnerabilities associated with these systems. This paper aims to detail the components of ICS, to identify security threats, to give some real-life examples of the incidents around the world, to draw attention to possible terrorists' use of the vulnerabilities and to offer recommendations towards more cyber-resilient critical infrastructure.

2. Architecture

Even though there are several types of ICS, such as Monolithic (based on standalone mainframes), Distributed (associated with a local area network to connect distributed operating stations), Networked (likewise Distributed SCADA but is oriented to commercial off-the-shelf systems), and IoT (integrated with IoT and cloud environment)[6]; almost all of them include Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS) as well as Programmable Logic Controllers (PLC).

---

[5] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security, 89.

[6] Asghar, M. R., Hu, Q. W., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165.

SCADA is widely used to control industrial processes locally or at remote locations and also to monitor, gather, and process real-time data. Known as a system of software and hardware elements, SCADA directly interacts with devices such as sensors, pumps, valves, motors, and through Human-Machine Interface (HMI)[7] software and also records events into a log file. These systems are crucial for industrial organizations because they maintain efficiency, process data for 'smarter' decisions, and communicate system issues to help mitigate downtime.

Over time, SCADA has undergone a significant evolution from a typically isolated environment to a highly interconnected network. This change has had numerous benefits, such as greater performance efficiency and the cost/price reduction of heavy equipment. However, the end result has been that SCADA is more vulnerable than before to various cyber-attacks.[8] To recognise vulnerabilities and potential threats it is very important to understand the architecture and to have information about the protocols regarding ICS.

SCADA uses a central computer system to retain and store information on local or remote devices to control industrial processes and facilities. The typical SCADA components can be classified according to their definitions, as illustrated in Fig. 1.

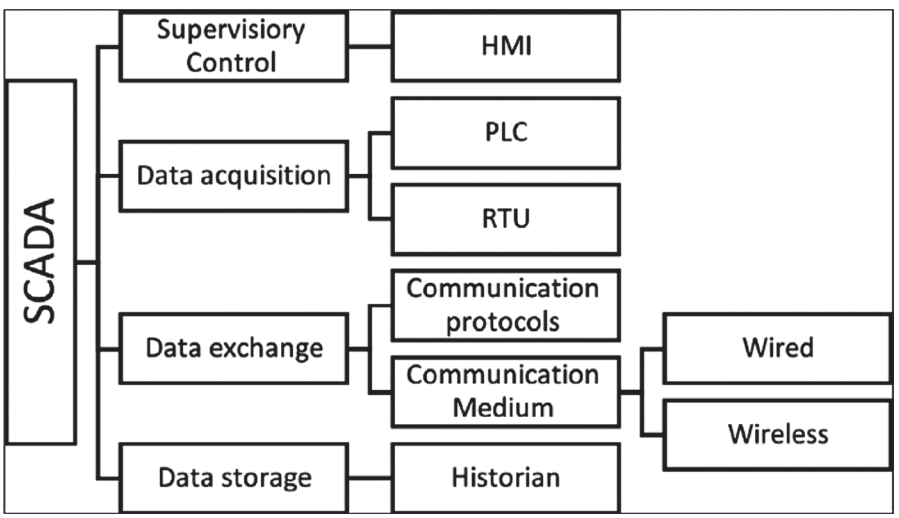

Figure 1: SCADA Components

7 The HMI is software and hardware that allows human operators to monitor the state of a process under control, modify control settings and manually override automatic control operations in the event of an emergency.

8 Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security, 125.

Supervisory control: It is the primary function of the Human-Machine Interface (HMI). HMI software is an interface that is accountable for the supervision of industrial processes. By contrast, a master terminal unit (MTU) is a central supervisory controller that communicates with lower-field devices, such as remote terminal units (RTUs), over the ICS network.

Data acquisition: Data can be acquired from a Programmable Logic Controller (PLC) and/or an RTU. A PLC is a solid-state device that facilitates decision making by continually controlling and monitoring local industrial physical processes A PLC utilizes sensors to track the current state of a process, based on the logic in the PLC, and then sends it to its respective control center to be graphically displayed by the HMI to the control operator.

Data storage: Most SCADA systems use a structured query language (SQL) database to store timestamped data. Integrated SCADA softwares is used to collect real-time data from various SCADA devices and stores it in a database, such as a SQL.

Data exchange: Communication protocols are used to exchange data between SCADA components.[9] More details about the SCADA communication protocols and cyber attacks are provided below.

3. Protocols

Initially, MTUs and RTUs communicated via a wired link, such as a dial-up modem interface but, since wired links are restricted to small-scale areas and networks, industry planners moved to more advanced protocols to achieve scalability. In a SCADA system, MTUs and RTUs communicate using a communication server and proprietary protocols such as Modbus-RTU, Profibus and DNP3.

MODBUS is the most widely used SCADA protocol. SCADA protocols are communications protocols designed for the exchange of control messages on industrial networks and have many vulnerabilities. These MODBUS/TCP protocol implementation vulnerabilities could allow an attacker to perform reconnaissance activity or issue arbitrary commands. Below are listed the basic sections/classes of MOSBUS/TCP protocol vulnerabilities:

a. *Lack of Confidentiality:* All MODBUS messages are transmitted in clear text across the transmission media.

9 ibid

b. *Lack of Integrity:* There is no integrity checks built into the MODBUS application protocol. As a result, it depends on lower layer protocols to preserve integrity.

c. *Lack of Authentication:* There is no authentication at any level of the MODBUS protocol. (One possible exception could be undocumented programming commands.)

d. *Simplistic Framing:* MODBUS/TCP frames are sent over established TCP connections. While such connections are usually reliable, they have a significant drawback. TCP connection is more reliable than UDP but the guarantee is still not complete.

e. *Lack of Session Structure:* Like many request/response protocols (SNMP, HTTP, etc.), MODBUS/TCP consists of short-lived transactions where the master initiates a request to the slave that results in a single action. When combined with the lack of authentication and poor TCP initial sequence number (ISN) generation in many embedded devices, it becomes possible for attackers to inject commands with no knowledge of the existing session.

PROFIBUS stands out from other fieldbus systems[10] because it offers an extraordinary breadth of applications. PROFIBUS can be used for fast and cost-effective production in a wide area of applications – such as factory, process or building automation. As an open standard, PROFIBUS is compatible with a wide range of components from different manufacturers. This protocol boasts further advantageous features, which include network components suitable for hazardous industrial environments; high security of investment, as existing networks can be extended without any adverse impacts; and high levels of operational reliability and plant availability, due to different diagnostic options. And although it is mainly used at the field level of an industrial network architecture, PROFIBUS can also be used at the control level. PROFIBUS is flexible, durable and safety-oriented, which contributes to its success and wide use.

However, the security 'holes' in PROFIBUS are concerning. Lack of authorization and authentication control means that a rogue device can be connected to and communicate on PROFIBUS, gaining access to the clear-text telegrams. In an attack tree analysis[11] of an industrial network segment that has a PROFIBUS

[10] A fieldbus is a serial bus system used in machines and systems to connect sensors and actuators (motors) to each other and to one or multiple masters (industrial PCs, PLCs). Fieldbuses make it possible to exchange data between different system components over long distances and under high external load.

[11] Attack trees are conceptual diagrams showing how an asset, or target, might be attacked. Attack trees have been used in a variety of applications. In the field of information technology, they have been used to describe threats on computer systems and possible attacks to realize those threats.

backbone, a connected controller is considered a prime target, as it is a device that can issue commands that will disrupt the functioning of the plant.

Typical attack goals include: gain access to the controller (master); disable; or write data that will compromise the master. With access to the master, an attacker can also gain access to slaves, to achieve goals as above, in addition to reading data from the slave or programming the slave.[12] Access to a controller allows an attacker to monitor the network communication, map the network topology and spoof and/or capture, interpret and use the commands observed. Once an attacker achieves network access, 'sniffing'[13] the network is a relatively easier task, especially where there is no confidentiality control in place. Such a network attack is possible through PROFIBUS, as it lacks authentication and authorization controls to verify connected masters, to validate the communication and restrict communication to legitimate components.

The infamous Stuxnet worm is an example of an attack that exploited these vulnerabilities. Stuxnet is a sophisticated piece of malware that was injected into the SCADA system at a uranium enrichment facility in Iran. This worm compromised PLCs, and whilst operating as a 'logic bomb'[14], monitored the clear-text communication on a PROFIBUS DP network, waiting for specific data before executing its payload.[15] Had authentication and authorization controls been in place on the PROFIBUS network, it is possible that this attack would not have been successful.[16]

DNP3 (Distributed Network Protocol) is a communication protocols used between components in process automation systems. It is used in communications between a master station and RTUs or IEDs (Intelligent Electronic Device). In DNP3 a three-layer Enhanced Performance Architecture (EPA) is created which includes a data link, transport, and application layer.

DNP3 faces various threats which includes eavesdropping (secretly listening to the message), man-in-the middle attack (attacker not only listens to the messages

---

12 Bryes, E., Franz, M. & Miller, D., (2004). 'The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems', International Infrastructure Security Survivability Workshop (IISW)

13 Sniffing is a process of monitoring and capturing all data packets passing through computer network.

14 A logic bomb is a set of instructions in a program carrying a malicious payload that can attack an operating system, program, or network.

15 Knapp, E.D. & Langill, J.T., (2015). Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, 2nd edn., Syngress (Elsevier), Massachusetts, USA.

16 Watson, V., Lou, X. & Gao, Y. (2017). A Review of PROFIBUS Protocol Vulnerabilities Considerations for Implementing Authentication and Authorization Controls. In Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, pages 444-449.

between parties but can also modify, delete, and replay the messages), spoofing (attacker pretends to be an authorized user) and replay (an attack that attempts to trick the system by retransmitting a legitimate message).[17]

4. Attacks on ICS

Cybersecurity in ICS has become a crucial topic due to the increasing number of cyber attacks targeting critical infrastructure. ICS have several advantages by combining SCADA with the IoT and a cloud environment, such as enhanced cost reduction, flexibility and performance efficiency.[18] However, the number of cyber threats against SCADA have risen rapidly due to increased remote access and internet connectivity. In extreme cases, the failure to protect SCADA from such attacks threatens human lives. ICS have a direct connection to an industrial process; intentional or unintentional security breaches can have serious consequences including the potential for loss or life and injury, environmental damage, loss of production and the compromise of operational safety.[19] In Table 1 publicly disclosed cyberattacks (between 1998-2020) targeting ICS can be seen.[20]

Table 1 Summary of attacks.

Attack	Date	Sector	Impact
PLC Password Change	1988	Manufacturing	Denial of control
Ignalina Nudear Power Plant	1992	Civil nuclear	Loss of productivity
Salt River Project	1994	Energy and water	Loss of productivity
Omega Engineering	1996	Manufacturing	Disk wipe
Worcester	1997	Transport	Loss of productivity, revenue, availability-
Gazprom	1999	Chemical & energy	Loss of productivity and revenue
Bradwell Nuclear Power Plant	1999	Civil nuclear	Disk wipe

[17] Bhagyashri Sangewar, B. & Buchade, A. R., (2020). Survey on Analysis of Security Threats in DNP3 Protocol, International Journal of Scientific & Technology Research Volume 9, Issue 06, June 2020, pages 365-369.

[18] Sajid, A., Abbas, H., Saleem, K., 2016. Cloud-assisted IOT-based SCADA systems security: a review of the state of the art and future challenges. IEEE 4.

[19] International Electrotechnical Commission, Industrial Communication Networks–Network and System Security – Part 1 1: Terminology, Concepts and Models, (2009). IEC/TS 62443-1-1 ed 1.0, Geneva, Switzerland.

[20] Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. International Journal of Critical Infrastructure Protection, 35.

Maroochy Water System	2000	Water	Damage to properiy
Cal-ISO System	2001	Energy	None disclosed
Virüs on Manufacturing System	2001	Manufacturing	Loss of productivity and revenue
Houston Port	2001	Transport	Loss of productivity and revenue
Gas Processing Plant	2001	Cherncal	Loss of productivity and revenue
PDVSA	2002	Chemical	Loss of productivity and revenue, disk wipe
Flight Pianning Computer	2003	Transport	Loss of productivity and revenue
CSX Train Signaling System	2003	Transport	Loss of productivrty and revenue
Contractor infects SCADA Network	2004	Food	Loss of productivity and revenue
Daimler Chrysler Plants	2005	Manufacturing	Loss of productivity and revenue
Tehama-Colusa Canal	2007	Water	Damage to property
LodzTram System Hacked	2008	Transport	Loss of safety
US Power Grid	2009	Energy	None disclosed
Hospital HVAC	2009	Health	Loss of safety
Night Dragon	2009	Energy	Theft of operational data
Sality Virüs infects DVS Servers	2009	Chemical	Loss of view
Stuxnet	2010	Civil nuclear	Damage to property, Manipulation of view and control
Shionogi	2011	Health	Disk wipe
Niagra AX	2012	Manufacturing	Manipulation of control
Espionage on Iranian CI	2012	Chemical	Theft of operational data, Unintentional disk wipe
Turbine Control System	2012	Energy	Loss of productivity and revenue, Theft of operational data
Rye Brook Dam	2013	Water and energy	None disdosed
European Public Utility Services	2014	Various	Denial of service, Theft of operational data
German Steel Mill	2014	Manufacturing	Damage to property
Ukrainian Energy	2015	Energy	Loss of productivity and revenue
Ukrainian Energy	2016	Energy	Disk wipe, loss of productivity and revenue.
Wolf Creek	2017	Civil nuclear	None disclosed
Cadbury Factory Attack	2017	Food	Loss of productivity and revenue
Triton/Petro Rabigh	2017	Chemical	Denial of control, Loss of safety
Norsk Hydro	2019	Manufacturing and energy	Loss of view
Triton/Undisclosed	2019	Undisclosed	Denial of control, damage to property, loss of safety
Hackers Target Oil Producers	2020	Chemical	Theft of operational data
Israeli Water Facilities Attacked	2020	Water	None disclosed
Cyber-attack on Shahid Rajaie Port	2020	Transport	Loss of productivity and revenue
Honda Factories Cyber Attack	2020	Manufacturing	Denial of control

These security incidents[21] [22] tell us that ICS security is closely connected with the real world, especially in power (including nuclear power), military, petroleum and petrochemical industry, rail transit, and other key infrastructures. Compared with traditional cyber attacks, which only bring economic losses to the victims or enterprises[23], ICS vulnerabilities may lead to unimaginable and catastrophic consequences, such as the uncontrollable explosion of nuclear power plants or power failure nationwide. As a result, ICS vulnerabilities can seriously affect industrial production, life and property safety in our daily lives.[24]

Due to their vulnerabilities, critical infrastructures can be penetrated through application exploits, backdoor attacks, exploitation of operating systems, unauthorized access, exploitation of system configurations, tampering, etc.[25] The sophistication of attacks utilizing advanced malware such as Stuxnet (2010), Nightdragon (2011), Flame (2012) and Dragonfly (2013) has proven that attackers possess the required resources, technical expertise, intention, and motivation to successfully compromise critical ICS.[26] [27]

5. Possible Terrorists' Usage

The term "cyber terror" appeared for the first time in the mid 1980's, and experts from wide range of fields have become interested the potential of cyber terrorism. This brings the incoherence of the definition of the term because experts have scrutinized from different perspectives such as international studies, law enforcement, information security, anti-terror etc.

According Akhgar, B., Staniforth, A., Bosco's 2014 study[28], a comprehensive

[21] J. Leyden. (2008) Polish teen derails tram after hacking train network, The Register, available at https://www.theregister.com/2008/01/11/tram_hack/ (accessed 25 February 2023).

[22] R. Langner. (2011) Stuxnet: Dissecting a cyberwarfare weapon, Security Privacy, IEEE 9 (3) 49–51.

[23] Kumar, R., Kela, R., Singh, S., & Trujillo-Rasua, R. (2022). APT attacks on industrial control systems: A tale of three incidents. International Journal of Critical Infrastructure Protection, 37.

[24] Asghar, M. R., Hu, Q. W., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165.

[25] Ismail, S., Sitnikova, E., & Slay, J. (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. Ict Systems Security and Privacy Protection, Ifip Tc 11 International Conference, Sec 2014, 428, 242-249.

[26] Miller, B., and Dale, R. (2012) "A survey SCADA of and critical infrastructure incidents." In Proceedings of the 1st Annual conference on Research in information technology, pp. 51-56. ACM.

[27] Symantec Security Response. "Dragonfly: Cyberespionage Attacks against Energy Suppliers". Symantec Security Response Version 1.21, (2014).

[28] Akhgar, B., Staniforth, A., Bosco, F. (2014) Cyber terrorism: Case studies. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 165–174). Elsevier Inc.

definition of cyber terrorism could be;

> *The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organization; made for the purposes of advancing a political, religious, racial or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorized actions affecting information and communication technology-based control of real-world physical processes; and it involves or causes:*
>
> • *violence to, suffering of, serious injuries to, or the death of (a) persons(s),*
> • *serious damage to a property,*
> • *a serious risk to the health and safety of the public,*
> • *a serious economic loss,*
> • *a serious breach of ecological safety,*
> • *a serious breach of the social and political stability and cohesion of a nation.*

Cyber terrorism in the SCADA Systems context is defined as the use of Information Communications Technology by terrorist groups and cyber threat actors to promote extremist or aggressive tendencies, usually politically motivated and designed to have a forceful or catastrophic impact. The perpetrator must use information systems or other electronic means to launch a cyber attack against critical information infrastructures. Also defined as "non-state actors' use of ICT to attack and control critical information systems with political motivation and the intent to cause harm and spread fear to people or at least with the anticipation of changing domestic, national or international events".[29]

Using the final definitions above, there are only a limited number of actions after the mid 1980s which may have approached a real cyber terror act. A first one was during the Nagorno-Karabakh conflict of 1999. Following unconfirmed reports, hackers modified blood types in patient records in a hospital database causing the risk of people dying through receiving the wrong blood transfusion. A second was the 2006–2007 preparations by an Al Qa'ida-related terrorist group which

---

[29] Ismail, S., Sitnikova, E., & Slay, J. (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks. ICT Systems Security and Privacy Protection, Ifip Tc 11 International Conference, Sec 2014, 428, 242-249.

planned to physically target the Telehouse telecommunications center and internet exchange in the London Docklands area. In August 2006, the potential societal effect of such an attack had been demonstrated by a small power disruption at Telehouse. This technical disruption took down tens of thousands of websites and hundreds of thousands of customers of Plusnet's internet services for a number of hours. The societal effects of a possible long-duration disruption which could have been the result of a successful physical attack can only be guessed at but thankfully would have been minor given the redundancy of systems, networks, backed-up information, and services[30].

What distinguishes the contentious politics of cyber terrorism from hacktivism is that the attack goes beyond inconveniencing its victims to result in physical violence against them or serious damage to property or critical infrastructure. Specific examples would include hacking attacks against SCADA systems and industrial controllers that allow perpetrators to breach a dam, thereby flooding a major urban area; computer attacks that derail passenger trains, causing them to crash; or attacks that wipe out the bank accounts, and life savings, of millions of customers. Critically, such violence and physical damage is not an end in itself but the means by which attackers seek to terrorize people beyond their immediate victims.

These four elements - computer generation, political motivation, physical violence, and psychological coercion - are the essential attributes of cyber terrorism. To qualify as cyber terrorism, an act must contain all four properties, the combination of which distinguishes it from its broader genus and other cyber attack species, such as hacktivism and cyber warfare.

Not a single cyber attack carried out to date contains the four attributes of cyber terrorism. This includes the many operations of Anonymous', Stuxnet, and al Qaeda, which has never carried out a major cyber attack, despite expressing a desire to do so.[31]

Also, cyber terrorism in the violent sense has never occurred[32]. There is no evidence of terrorists resorting to computers to kill or destructively disrupt societies

---

[30] Akhgar, B., Staniforth, A., Bosco, F. (2014) Cyber terrorism: Case studies. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 165–174). Elsevier Inc.

[31] Kenney, M. (2015) Cyber Terrorism in a Post-Stuxnet World, Orbis, Volume 59, Issue 1, Pages 111-128,

[32] Conway, M. (2014) "Reality Check: Assessing the (Un) Likelihood of Cyberterrorism," *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald New York: Springer, 103–121.

and most scholars think it is unlikely they will do so any time soon.[33] However, given the reality of terrorism (especially constant exploitation of new and emerging technologies), and the possibility of cyber terrorism, countries should be prepared for potential attacks on ICS in a way that makes countries more resilient against cyber attacks.

6. Resilience in Critical Infrastructure

According to Gartner, a resilient cybersecurity strategy is essential to running a business (or other form of operation) while protecting against security threats and preventing data breaches and other enterprise cybersecurity threats. [34] In such a strategy there are so many features that have to be taken into account, namely business continuity, disaster recovery, crisis management, supply chain risk management, cyber and physical security, incident reporting, information sharing etc.

Cybersecurity measures have been implemented to protect control systems and networks from cyber attacks. However, no system can be completely secure, and the potential for attacks on power plants remains a concern for governments and industry organizations. It is important for critical infrastructures to continuously assess and improve their security measures to reduce the risk of successful attacks.

Preventing undesirable incidents from occurring in an industrial control environment is difficult because sensors, actuators, controllers and networks will all experience failures at some point. Since incidents are unlikely to be eliminated entirely, it is necessary to minimize their impacts instead.[35] Hence, cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. The ability to continuously deliver the intended outcome can pertain to not only to a nation/institution, but also an organization or even a specific IT system.[36]

---

[33] Jarvis, L. and Macdonald, S. (2015) "What Is Cyberterrorism? Findings from a Survey of Researchers," *Terrorism and Political Violence* 27, no. 4: 657–78; Jian Hua and Sanjay Bapna, "Economic Impact"; Armenia and Tsaples, "Individual behavior"

[34] "The IT Roadmap for Cybersecurity", Gartner, available at https://www.gartner.com/en/information-technology/trends/the-it-roadmap-for-cybersecurity (accessed 20 January 2023)

[35] Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (2017). Improving the cyber resilience of industrial control systems. *International Journal of Critical Infrastructure Protection*, *17*, 30-48.

[36] Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). Cyber Resilience - Fundamentals for a Definition. Advances in Intelligent Systems and Computing. Vol. 353. Stockholm University. pp. 311–316.

Resilient control systems are designed so that the impacts of undesirable events are minimized. Zhu et al.[37]list five criteria for measuring the resilience of a control system:

- *Protection time:* The time that a system can withstand an incident without performance degradation.
- *Degradation time:* The time that a system takes to reach its maximal performance disruption due to an incident.
- *Identification time:* The time that a system takes to identify an incident.
- *Recovery time:* The time that a system needs to recover (e.g., return to normal operation) after an incident.
- *Performance degradation:* The maximal system performance disruption due to an incident.

In the United States of America, President Bush created the President's Critical Infrastructure Protection Board in October 2001 through Executive Order 13231[38] to coordinate all federal activities related to the protection of information systems and networks supporting critical infrastructures. The Department of Energy plays a key role in protecting the critical energy infrastructure of the nation as specified in the National Strategy for Homeland Security. In fulfilling this responsibility, the Secretary of Energy's Office of Independent Oversight and Performance Assurance has conducted a number of assessments of organizations with SCADA networks to develop an in-depth understanding of SCADA networks and steps necessary to secure these networks.

The President's Critical Infrastructure Protection Board, and the Department of Energy, have developed the steps outlined to help any organization improve the security of its SCADA networks[39]. These steps (Table 2) are not meant to be prescriptive or all-inclusive. However, they do address essential actions to be

---

[37] Zhu, Q., Wei D. and Ji, K. (2016) Hierarchical architectures of resilient control systems: Concepts, metrics and design principles, in *Cyber Security for Industrial Control Systems: From the Viewpoint of Closed-Loop* , P. Cheng, H. Zhang and J. Chen (Eds.), CRC Press, Boca Raton, Florida, pp. 151–182.

[38] "Executive Order 13231 of October 16, 2001. Critical Infrastructure Protection in the Information Age", The Department of Homeland Security (DHS), available at https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf (accessed 25 February 2023)

[39] "21 Steps to Improve Cyber Security of SCADA Networks", The Department of Energy, available at https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (accessed 25 February 2023)

taken to improve the protection of SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.

SCADA Security Policy includes, security policy, organization information security, human resource security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, incident management, SCADA business continuity management and finally SCADA compliance.[40] Nations also have regulations, strategies and policies to make their critical infrastructures resilient.

Table 2 21 Steps 1o Improve Cyber Securtiy of SCADA Networks

1. Identify all connections to SCADA networks
2. Disconnect unnecessary connections to the SCADA network
3. Evaluate and strengthen the security of any remaining connections to the SCADA network
4. Harden SCADA networks by removing or disabling unnecessary services
5. Do not rely on proprietary protocols to protect your system
6. Implement the security features provided by device and system vendors
7. Establish strong controls over any medium that is used as a backdoor into the SCADA network
8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring
9. Perform technical audits of SCADA devices and networks, and any other connected networks, to idenfitfy security concers
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluale their security
11. Establish SCADA "Red Teams to identify and evaluate possible attack scenarios
12. Clearly define cyber security roles, responsibilities and authorities for managers, system administrators, and users
13. Document network architecture and systems that serve critical functions or contain sensitive information thet require additional levels of protection
14. Establish a rigorous, ongoing risk management process
15. Establish a network protection strategy based on the principle of defense-in-depth
16. Clearly identify cyber security requirements
17. Establish effective configuration management processes
18. Conduct routine self-assessments
19. Establish system backups and disaster recover plans
20. Senior organizational leadership should establish expectations security performance and hold individuals accountable for their performance
21. Establish policies and conduct training to mnimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

---

40 Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1), 23-40.

In the United Kingdom, the Center for the Protection of National Infrastructure (CPNI) provided a framework[41] for protecting process control systems from electronic attack. This framework is based on industry good practice from process control and IT security and focuses on seven key themes (Fig 2).

- Understand the business risks
- Implement secure architecture
- Establish response capabilities
- Improve awareness and skills
- Manage third party risks
- Engage projects
- Establish ongoing governance.

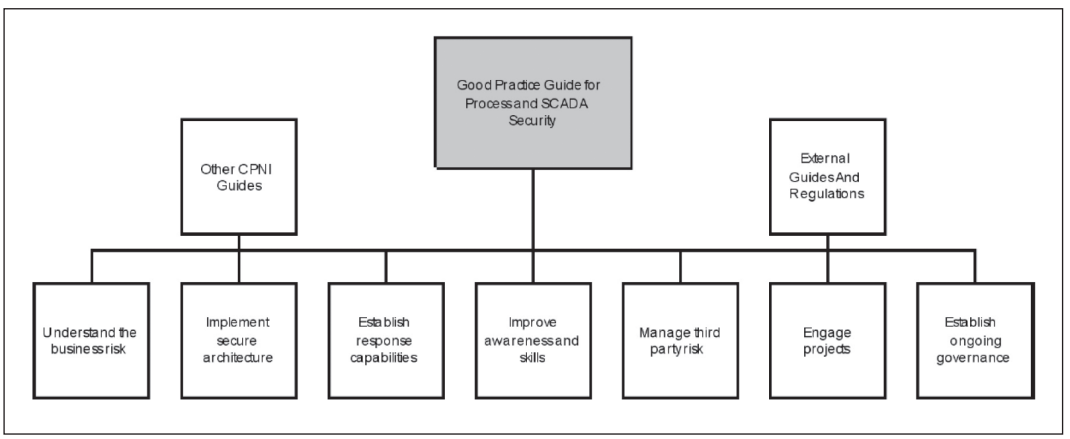

Figure 2 Good Practice Guide framework

The National Institute of Standards and Technology (NIST) of United States Department of Commerce, provides guidance on how to secure Industrial Control Systems with an effective cybersecurity program for an ICS should apply a strategy known as “defense-in-depth,” layering security mechanisms such that the impact of a failure in any one mechanism is minimized. Organizations should not rely on “security by obscurity.”

[41] “Good Practice Guide Process Control and Scada Security”, Center for the Protection National Infrastructure (CPNI) available at http://osgug.ucaiug.org/conformity/security/SharedDocuments/Reference/UK-CPNI-GPG-GuideImplementSecureArchitecture.pdf (accessed 21 February 2022)

In a typical ICS this means a defense-in-depth strategy that includes:

- *Developing security policies, procedures, training and educational material that applies specifically to the ICS.*
- *Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.*
- *Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.*
- *Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.*
- *Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).*
- *Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks).*
- *Ensuring that critical components are redundant and are on redundant networks.*
- *Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.*
- *Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.*
- *Restricting physical access to the ICS network and devices.*
- *Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).*
- *Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).*
- *Using modern technology, such as smart cards for Personal Identity Verification (PIV).*
- *Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.*
- *Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.*

- *Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.*
- *Tracking and monitoring audit trails on critical areas of the ICS.*
- *Employing reliable and secure network protocols and services where feasible*[42]*.*

Although there is no common understanding on resilience in the cybersecurity of critical infrastructures, the most important thing is to be resilient from the organizational point of view.

7. Conclusion

In this section you may find the summary of the aforementioned guidance, strategies, policies etc. and suggestions to defend critical infrastructures from the cyber attacks and cyber actors especially cyber terrorists

Industrial Control Systems are one of the most important part in today's industry, because they support automation, distributed control, and process monitoring from remote locations. Given that they are one the most valuable components of the Critical Infrastructure of a nation, it is important to defend its security by all means necessary. Initially designed to be used in distributed and isolated areas, ICS have been forced to be connected to a network or to other systems via specialized communication mechanisms or protocols. This places critical infrastructures at risk of being a victim of cyber attacks.

Cyber space, cyber actors and attack vectors are constantly changing, so that threats to industrial control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. Potential threats to ICS should be measured, analyzed and monitored to protect the interest of the public, stakeholders, employees, vendors, customers, broader society, and the nation as a whole according to risk management policy. Risk analysis is, therefore, necessary to take decisions to make critical infrastructures resilient.

To protect data and critical assets in critical infrastructures, some technical regulations must be put in place. Network segmentation and segregation (namely

[42] Keith Stouffer, K., Pillitteri, V., Lightman S., Abrams, M., Hahn, A. (2015) "Guide to Industrial Control Systems (ICS) Security" NIST Special Publication 800-82 Revision 2

physical and logical separation) to reduce access sensitive information, network traffic filtering, boundary protection measures, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) are some of the technical requirements that managers should plan in detail. A multi-layer strategy involving two or more different overlapping security mechanisms, also known as defense-in-depth, is desirable in critical infrastructures.

After setting a technical baseline, independent reviews and audits should be executed regularly. This includes the examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. Also, configuration management is required for policies and procedures to control modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Personnel security awareness is also required since security awareness is a critical part of ICS incident prevention, particularly when it comes to social engineering. Organizations should design effective training and awareness programs and communication mechanisms to help employees understand why regulations are required. Training programs also demonstrate management's commitment to, and the value of, a cybersecurity program.

Regardless of the steps taken to protect critical infrastructures, there is always a possibility of compromise by an intentional or unintentional incident. Incident response should include policies and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services. To minimize the effects of intrusions, it is also necessary to have a response plan.

BIBLIOGRAPHY

Akhgar, B., Staniforth, A., Bosco, F. (2014) Cyber terrorism: Case studies. *In Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 165–174). Elsevier Inc.

Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2023). SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security.

Asghar, M. R., Hu, Q. W., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks.

Bhagyashri Sangewar, B. & Buchade, A. R., 2020, Survey on Analysis of Security Threats in DNP3 Protocol. *International Journal of Scientific & Technology Research* Volume 9, Issue 06, June 2020.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security.

Bryes, E., Franz, M. & Miller, D. (2004). The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. *International Infrastructure Security Survivability Workshop* (IISW).

Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). Cyber Resilience - Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*. Vol. 353. Stockholm University.

Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (2017). Improving the cyber resilience of industrial control systems. *International Journal of Critical Infrastructure Protection*, *17*.

Conway, M. (2014). Reality Check: Assessing the (Un) Likelihood of Cyberterrorism. *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald New York: Springer.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. Survival, 53(1).

International Electrotechnical Commission, Industrial Communication Networks–Network and System Security – Part 1 1*: Terminology, Concepts and Models*, IEC/TS 62443-1-1 ed 1.0, Geneva, Switzerland, (2009).

Ismail, S., Sitnikova, E., & Slay, J. (2014). Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber Terrorist Attacks. *ICT Systems Security and Privacy Protection,* Ifip Tc 11 International Conference, Sec 2014, 428.

Jarvis, L. and Macdonald, S. (2015). What Is Cyberterrorism? Findings from a Survey of Researchers. *Terrorism and Political Violence* 27, no. 4 (2015): 657–78; Jian Hua and Sanjay Bapna, "Economic Impact"; Armenia and Tsaples, "Individual behavior".

Keith Stouffer, K., Pillitteri, V., Lightman S., Abrams, M., Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82 Revision 2.

Kenney, M. Cyber-Terrorism in a Post-Stuxnet World, Orbis, Volume 59, Issue 1, 2015.

Knapp, E.D. & Langill, J.T., (2015). *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd edn., Syngress (Elsevier), Massachusetts, USA.

Kumar, R., Kela, R., Singh, S., & Trujillo-Rasua, R. (2022). APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, 37.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon, Security Privacy, IEEE 9 (3).

Miller, B. and Dale R. (2012). A survey SCADA of and critical infrastructure incidents. *In Proceedings of the 1st Annual Conference on Research in Information Technology,* pp. 51-56. ACM.

Miller, T., Staves, A., Maesschalck, S., Sturdee, M., & Green, B. (2021). Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection.*

Sajid, A., Abbas, H., Saleem, K., (2016). Cloud-assisted IOT-based SCADA systems security: a review of the state of the art and future challenges. IEEE 4.

Symantec Security Response. “Dragonfly: Cyberespionage Attacks against Energy Suppliers”. Symantec Security Response Version 1.21, (2014).

Zhu, Q., Wei D. and Ji, K. (2016). Hierarchical architectures of resilient control systems: Concepts, metrics and design principles. *Cyber Security for Industrial Control Systems: From the Viewpoint of Closed-Loop*, P. Cheng, H. Zhang and J. Chen (Eds.), CRC Press, Boca Raton, Florida.

Watson, V., Lou, X. & Gao, Y. (2017). A Review of PROFIBUS Protocol Vulnerabilities Considerations for Implementing Authentication and Authorization Controls. *In Proceedings of the 14th International Joint Conference on e-Business and Telecommunications* (ICETE 2017) - Volume 4: SECRYPT.

http://osgug.ucaiug.org/conformity/security/SharedDocuments/Reference/UK-CPNI-GPG-GuideImplementSecureArchitecture.pdf (accessed 21 February 2022).

https://irp.fas.org/offdocs/pdd/pdd-63.htm (accessed 21 December 2022).

https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf (accessed 25 February 2023).

https://www.gartner.com/en/information-technology/trends/the-it-roadmap-for-cybersecurity (accessed 20 January 2023).

https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf (accessed 25 February 2023).

https://www.theregister.com/2008/01/11/tram_hack/ (accessed 25 February 2023).

Defence Against Terrorism
Review DATR Magazine

E-DATR, 2023; 18 : 67-90
Electronic Online ISSN 1307 - 9190
https://dergipark.org.tr/tr/pub/datr

Representations of Political Violence in Digital Media: Evaluating Media Coverage of the Assassination of Japan's Former Prime Minister Shinzo Abe

Naz Almaç[1]

Abstract

It's crucial to define what political violence is and its various forms. It's also important to discuss the impact of such violence on societies, governments, and the media. This article investigates political violence and terrorism in the digital media. To examine the topic, this article adopts the communication perspective framing theory because it demonstrates how political violence framed and conveyed through digital media and how rhetorical strategies used by media companies can persuade readers. A literature review that explores into the complex relationship between media and acts of terrorism or political violence is presented. Douglas Kellner concludes that after September 11 attacks both U.S and Islamic Jihadists used the media to promote their agenda and criticizes hegemonic political narrative of "good versus evil" and "us versus them"[2]*. With this in mind, this paper analyses the media coverage of the assassination of Japan's former Prime Minister Shinzo Abe in digital media was examined through framing theory and content analysis has been chosen as a methodology. The chosen case study provides a concrete example in which to apply*

1 Research Assistant Naz Almaç, Başkent University, nalmac@baskent.edu.tr

2 Kellner, D. (2004). 9/11, spectacles of terror, and media manipulation: A critique of Jihadist and Bush media politics. Critical Discourse Studies, 1(1), 41-64.

the theories and concepts discussed in literature review as; analyzing this specific event in detail illustrates the nuances of representation in digital media. As part of this analysis it is crucial to define what political violence is and its various forms. It is also important to discuss the impact of such violence on societies, governments, and the media. This article investigates political violence and terrorism in the media. To examine the topic, this article adopts the communication perspective framing theory because it demonstrates how political violence framed and conveyed through digital media and how rhetorical strategies used by news media outlets can persuade readers. A literature review that delves into the complex relationship between media and acts of terrorism or political violence is presented. In this media ecosystem it is rather difficult to present violence events objectively without thinking about the international relations of countries where the media outlets reside. To explore different perspectives on the topic, Western and Eastern digital media companies had been chosen. The selected news coverage and the coding scheme applied highlights the differences between Western and Eastern digital media coverages of the event.

Keywords: *Terrorism, Digital Media, Framing Theory, Political Violence, Communication*

Introduction

In digital media, terrorism or acts of political violence are frequently represented in a variety of ways, including news stories, photographs, videos, and social media posts. How people perceive and react to acts of terrorism can then be significantly influenced by these representations. The majority of information about terrorist incidents is found in news articles, which intend to normally written factually and neutrally. Yet news organizations can utilize sensational language or visuals to draw readers, which might result in the spread of fear. On the other hand, cultural differences also affect the framing of terror events in media. Compared to traditional media, digital media environments have the capability of facilitating a two-way communication[3] so, in this way, extremists and terrorist groups begin to attract their

[3] According to Shannon and Weaver (1948), the mathematic al model of communication refers to one-way communication however in recent years this model has been discussed because of the complex interaction between texts and the audience. In two-way communication model, the receiver of the text can give feedback.

audiences, often in real time[4]. Thus these groups builds a narrative to promote their agenda through digital media which opens a dialogue between the sender and receiver of the information.

The categorization of terror events and terrorism had been conceptualized diversely in previous literature[5]. However, whether these frameworks are also valid in mass media is debatable[6]. Alex Schmid states that one cannot comprehend terrorism solely through the lens of violence, we should also understand it through propaganda. As media texts use persuasion to convince their audience, it is crucial to understand terrorism in terms of communication. In this way, the literature review presented in the article maintains a scholarly approach to terrorism and it's the relationship with the media. Additionally, news outlets or news reporting's/stories discuss terror events and present framed text and photographs to the public. Thus, the event portrayed by the news becomes a representation of reality.

Terrorism mainly uses violence to encourage fear in the public. Furthermore, terrorists also use mass media to propagate that fear emotionally. The contemporary mass media landscape is crucial for understanding the news media's presentation of domestic violent events, news editors are an important part of this relationship as they frame these events and share it with public. As violent events portrayed on news are a symbolic representation of reality it is important to understand news outlets' framing of such an event. Japanese politician Shinzo Abe was the Prime Minister of Japan: on 8 July 2022 he was assasinated while delivering a campaign speech. He was a member of the Liberal Democratic Party (LDP) both his family and himself were involved in Japanese politics for many years. During his career, he is best known for the economic policies which are called "Abenomics". Through monetary easing and structural reforms, he had a profound impact on Japan's economy. After the assassination, a man called Tetsuya Yamagami was arrested immediately and charged with murder. The suspect confessed that he had been killed the Prime Minister Shinzo Abe with a homemade gun. According to the statement given by him, he believed that the Prime Minister was connected to the Unification Church. Yamagami said that the religious group brainwashed his mother thus the Prime Minister had a role in the spread of the religion in Japan.

---

4 Ashraf, A., & Foggett, S. Media and Counter-terrorism. COUNTER TERRORISM, 127.

5 Schmid, A. (2004). Terrorism-the definitional problem. Case W. Res. J. Int'l L., 36, 375.

6 Schmid, A. P. (2004). Frameworks for conceptualising terrorism. Terrorism and political violence, 16(2), 197-221.

Understanding the framing of news outlets is essential to untangle how violence is portrayed in the news media. To examine this event, six cross-cultural media companies were chosen and digital news stories that covered the event between 8 July 2022 and 31 December 2022 were analyzed with content analysis methodology. The chosen media companies are Pacific media companies which represent the West and East. Lastly, the initial reporting of the event by digital media companies chosen to further understand the news covering and representation of terror events in media. A coding scheme is constituted by the author to analyze and interpret the obtained data.

In the article, the notion of terrorism is studied within the scope of academic circles, NATO, and its representation by news outlets. Relevant communication theories on the subject and the relationship between media coverings and terror events will be examined thoroughly.

This article seeks to address the questions: Do media have shared definitions of representing acts of political violence? Do cultural differences and international relations of companies affect the covering of political violence acts and in turn change the news framing? To answer these questions, news presentation of terror will be examined through content analysis and the framing theory. News companies' stances on the event and allegations about the act will be examined. To actively interpret the obtained data rather than passively focus coding had been chosen for the methodology of the research.

The Notion of Terror and Political Violence

Terrere, a Latin word, is the etymological origin of the word 'terror' or 'fear'[7]. Leviathan author Thomas Hobbes defined terror as the fear of (violent) death[8]. In the 18th century, the French Revolution prepared the basis of the notion of terror. In this way, the modern usage of the term exists as early as the 12th century. Terror is defined as a war or harm against non-combatants during peacetime and commonly aided by religious or political reasons[9]. In literature, an act of violence is considered a terror event when the activity is driven by ideological purposes. The criminal violence against civilians exposes fear and conflict in society. Although

7 https://www.nytimes.com/2001/09/23/magazine/the-way-we-live-now-9-23-01-on-language-infamy.html

8 Hobbes, T. (1967). Hobbes's leviathan. Рипол Классик.

9 https://www.coe.int/en/web/compass/war-and-terrorism

there isn't any universal definition of terror, the scholarly approach to the notion creates a degree of mutual understanding of its uses and scope. Furthermore, organizations like the United Nations and NATO accept academic definitions of terrorism created by scholars[10] [11]. NATO defines terrorism as:

> "*The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives*"[12].

Terror and terrorism are generally thought to represent similar meanings. However, if terror is defined as harming civilians, terrorism represents these harms systematically[13]. Generally, in definitions of terrorism scholars address the notion as "harming civilians for ideological purposes"[14]. However, several academics say that this definition centering itself on harming can be ambiguous on some events[15]. For example, according to Alex P. Schmid; (2011) terrorism has almost a hundred definitions, because of this, it is difficult for people to agree on the definition of terrorism or the parameters of that definition. According to C. A. J. Coady[16], the definition of terrorism is a *"problem that cannot be solved"* since *"its natural home is in polemical, ideological, and propagandist contexts."* However, Rapoport's analysis of modern terrorism where four main stages are examined allows us to develop a common understanding of the term[17]. Although some scholars state that modern terrorism started with the French Revolution[18], Rapoport believes that modern terrorism began existing in 1880 in Russia. The four waves that had been examined by Rapoport are as follows: The Anarchist wave (1878–1919), the Anti-Colonial wave (1920s–early 1960s), New Left wave (mid-1960s–1990s), lastly the Religious wave (1979–ongoing). In the terror studies domain, Rapoport's research

---

10 https://www.nato.int/cps/en/natohq/topics_77646.htm

11 https://www.un.org/counterterrorism/

12 https://www.nato.int/cps/en/natohq/topics_69482.htm

13 Schmid, A. P. (2011). The definition of terrorism. In The Routledge handbook of terrorism research (pp. 39-157). Routledge.

14 İbid.

15 Saunders, B. (2008). Acts of self-harming protest and the definition of terrorism.

16 Coady, C. A. J. (2021). The meaning of terrorism. Oxford University Press.

17 Rapoport, D. C. (2019). The four waves of modern terrorism. In Transnational Terrorism (pp. 3-30). Routledge.

18 Erlenbusch, V. (2015). Terrorism and revolutionary violence: The emergence of terrorism in the French Revolution. Critical Studies on Terrorism, 8(2), 193-210.

has been very influential and valuable for the field of terrorism studies. Another highly influential article is Tom Parker and Nick Sitter's *The Four Horsemen of Terrorism: It's Not Waves, It's Strains*[19]. According to scholars we have been living in a time of terrorism for the past 150 years. The development of radical ideologies that encouraged revolutionary groups to experiment with new forms of political violence, as well as the significant advancements in mass communication and weapons technology in the nineteenth century, are all factors that contributed to the emergence of modern terrorism[20]. In this way, modern terrorism also has been exacerbated through mass communication.

Political violence, on the other hand, is a type of violence that is committed to achieve certain political goals[21]. The context of the notion varies because of the complex understanding of the term. Although politically violent acts can occur between states, non-state actors also use several strategies to attract an audience. In this way, it can also refer to violent non-state actors who target a state with politically motivated violence.

Numerous politically motivated militant, insurgent, extremist, and/or fundamentalist groups and individuals are convinced that the political systems and states in which they live will never give in to their demands[22], and as a result, they think that the only way to overthrow and/or reshape the government or state by their political and/or religious worldview is through violent means, which they regard as not only justified but also necessary to achieve their goals[23].

Communication Theories to Understand Violence in Digital Media

The Latin verb "communicare," which means "to share" or "to make common," is the root of communication. Communication can be defined as an information exchange between humans and animals[24]. The transfer of information is the standard definition of communication. In this case, a message is transmitted from a sender to

19 Parker, T., & Sitter, N. (2016). The four horsemen of terrorism: It's not waves, it's strains. Terrorism and Political Violence, 28(2), 197-216.

20 İbid.

21 Bosi, L., & Malthaner, S. (2015). Political violence. The Oxford handbook of social movements, 440-451.

22 Van Prooijen, J. W., & Kuijper, S. M. (2020). A comparison of extreme religious and political ideologies: Similar worldviews but different grievances. Personality and Individual Differences, 159, 109888.

23 İbid

24 Calhoun, C. (2012). Communication as a Social Science (and more). Intercom: Revista Brasileira de Ciências da Comunicação, 35, 277-310.

a recipient through a medium, such as sound, paper, physical motion, or electricity. As media such as television, and social media have evolved with technological developments; communication theories that analyze these channels have grown in parallel. Agenda Setting theory was developed by Maxwell McCombs and Dr. Donald Lewis Shaw[25], using the foundational work done by Walter Lippmann[26] as early as 1920's. The hypothesis made by these communication scholars, which has been extensively researched and applied to different media, contends that the media can influence public opinion by selecting which topics receive the greatest attention. The public, in Lippmann's opinion, reacts to "the pictures in our thoughts," or what he refers to as the pseudo-environment, rather than actual happenings in the environment[27]. The media intervenes and sets the agenda by providing more basic frameworks through which people might make sense of the world.

In 1963, Bernard Cohen followed Walter Lippmann's book *Public Opinion* (1922) and developed the Agenda-Setting theory. According to him, media or the press *"may not be successful much of the time in telling people what to think, but it is stunningly successful in telling its readers what to think about. The world will look different to different people" [28]*. Cohen's work later influenced McCombs and Shaw's interpretation of agenda-setting theory. Conflict, terrorism, crime, and drug crises within the United States are frequently the stories having the greatest influence on the news agenda of U.S.[29]. The absence of the United States and politics on news agenda are associated negatively with public opinion.

In Chapel Hill, North Carolina, during the 1968 presidential election, McCombs and Shaw introduced the idea of agenda-setting. By contrasting the hot topics on the media agenda with those that are important to voters who are still unsure, they looked at Lippmann's theory about how our mental images are built through the media[30]. In this way, they concluded that the undecided voters were affected by the agenda. The power of mass media and its impact on the public agenda was first empirically analyzed in the field of communication by McCombs and Shaw.

---

25 McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. Public opinion quarterly, 36(2), 176-187.

26 Lippmann, W. (2017). Public opinion. Routledge.

27 İbid.

28 Cohen, B. C. (2015). Press and foreign policy (Vol. 2321). Princeton university press.

29 Wanta, W., & Hu, Y. W. (1993). The agenda-setting effects of international news coverage: An examination of differing news frames. International Journal of Public Opinion Research, 5(3), 250-264.

30 Coleman, R., McCombs, M., Shaw, D., & Weaver, D. (2009). Agenda setting. In The handbook of journalism studies (pp. 167-180). Routledge.

Although developed for television studies primarily, cultivation theory is another communication theory that examines the effects of media. It implies that people who regularly consume particular media for extended periods interpret social reality as it is similarly portrayed in the media they consume, which then affects their attitudes and behaviors (Nabi, Riddle 2008). George Gerbner first developed the framework in the 1960's and the main hypothesis of the theory is that television content which is viewed by the public creates a terrifying world in people's minds more than it is. The thesis claims that *"the more time people spend 'living' in the television world, the more probable it is that they would assume that social reality matches with reality portrayed on television"*[31].

According to Gerbner; there are three types of analysis in the framework of Cultivation Theory; firstly *institutional process analysis, message system analysis,* lastly *Cultivation Analysis*[32]*.* The institutional process is defined as the analysis of the content distributors such as news media and television channels. Message system analysis is the analysis of the content of the information or the distributed message. Lastly, Gerbner looks at the longitudinal effects of these messages on people through surveys presenting the media reception of the audience. The cultivation theory was developed as a tool to examine how people were affected by television, particularly how being exposed to violent content on television affected viewers.

These communication theories help researchers to understand messages of the news content and understand the meaning behind both text and images that have been used for giving information to the public. In this way, in social sciences, another well-known theory is framing theory[33]. Framing describes how news media coverage affects public opinion in the communication process. At least three primary sets of influences have traditionally been identified by frame-building studies as having the potential to affect how journalists frame a particular issue: characteristic of the medium (IE digital vs. analog), political orientation of the media company, and time that has passed after the covered event. Frame theory has been studied by various scholars from different fields: however, compared to the studies by other scholars, Ervin Goffman is highly influential because of integrating cultural values

---

31 Nabi, R. L., & Riddle, K. (2008). Personality traits, television viewing, and the cultivation effect. Journal of Broadcasting & Electronic Media, 52(3), 327-348.

32 Gerbner, G., Gross, L., Morgan, M., & Signorielli, N. (1986). Living with television: The dynamics of the cultivation process. Perspectives on media effects, 1986, 17-40.

33 Goffman, E. (1974). Frame Analysis Cambridge. Mass.: Harvard Univ.

into the theory[34]. When Erving Goffman proposed that the meaning of a frame has implicit cultural foundations, he focused on the influence of the cultural environment in shaping frames[35]. In this way, theoretically, news that has been produced from different countries will have different framing attitudes because of national culture. In the communication process, frames can be found in four different places: the communicator, the text, the recipient, and the culture itself.

Van Dijk (1996,1998) states that written resources such as newspaper articles have a major influence on both everyday readers but also institutional actors, such as politicians and corporate executives. In this way in modern societies media functions as a powerful communicative tool for formulating a perspective of the world. Journalists covering news events transform the meaning of the events as they choose certain words and images[36]. In a way journalists also cover certain events to be significant for a large audience: this aspect of media coverage also turns complex reality into simple artifacts. As early as 1922 Walter Lippmann already understood that mass communication affects public opinion in a great way.

Globalization also influences media framing of news events: for example, hyper globalizers state that the contemporary society and the public sphere, in general, turned into a global village as theorized by Marshal McLuhan (1960). The globalization of the public sphere allows the global audience to receive the same news events. In this space large news conglomerates owns all the stories or narratives that had been produced by journalists. On the other hand, several scholars state that media produces traditional cultural texts rather than a global international perspective[37].

Communication research places framing theory in a position of importance starting in the 1990's. According to Entman (1993), framing is the process of choosing "aspects of a perceived reality and making them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described"[38]. The definition indicates that the nature of framing theory

34 Goffman, E. (1974). Frame Analysis Cambridge. Mass.: Harvard Univ.

35 İbid.

36 Ruigrok, N., & Van Atteveldt, W. (2007). Global angling with a local angle: How US, British, and Dutch newspapers frame global and local terrorist attacks. Harvard International Journal of Press/ Politics, 12(1), 68-90.

37 Hartley, J. (2012). Communication, cultural and media studies: The key concepts. Routledge.

38 Entman, R.M. 1993. "Framing: Towards Clarification of a Fractured Paradigm."Journal of Communication43(4):51–85

is complex. In this way, the selection, salience, and recommendation of certain events in news reports are important factors, and both the communicator and the audience are major parts of this communication process. Entman also notes that (1993) the communicator, the text, the receiver, and the culture are four possible topics of framing studies. Entman concludes that frame studies form a division in terms of studying the media frames and audience frames.

Popular narratives influence news and shape social and cultural identity. In this way, the discussions conducted by news outlets include several factors. Moreover, culture can be listed as an important factor in framing political violence in the news media.

Media and Terrorism

The following section introduces the methodology of the case study and examines the assassination of Japan's Prime Minister Shinzo Abe from Eastern and Western digital news companies. In communication studies, the term media defines the tools that spread information through various methods (electronic, printed, etc.). Among the first examples of such a process are the paintings found in the caves of France and Spain. Similar paintings are also found in Sulawesi Island in Indonesia. The motivation behind these paintings is still under debate: some scholars believe they are made to educate the next generations[39], and some believe they have ritualistic value[40]. Regardless of the motivation behind their creation, one thing is clear, they have become agents in the spreading of the information and kept this position even thousands of years after their creators have vanished. This aspect of the cave paintings renders them the first examples of mass media; media which can reach large masses of people.

Many cultural and technological developments have improved the reach of the media, like the adoption of the alphabet (especially phonetical) or the invention of paper. But two interconnected developments revolutionized the development of mass media as we know it: the ability to mass produce the information medium and the ability to consume it. Gutenberg's printing press allowed the mass production of texts and fueled the spread of literacy. Eventually, the developments sustained by literacy (with many other developments) paved the way to the Industrial Revolution

[39] Bronowski, J. (2011). The ascent of man. Random House.

[40] Whitley, D. S. (2009). Cave paintings and the human spirit: The origin of creativity and belief. Prometheus Books.

in the second half of the 18th century. As the Industrial Revolution developed, the masses became able to create time for the education of the young and even some time for leisure activities, which historically had only been available to the upper classes. This increase in education and the invention of free time for ordinary people strengthened the media and transformed it into the mass media we know and consume today. The invention of film, radio, television, the Internet, and smart devices further contributed to the developments and made mass media an indispensable part of our everyday experiences.

The power of mass media is immense and far-reaching. Mass media includes various forms of communication, such as television, radio, newspapers, magazines, the Internet, and social media platforms. Through mass media, information can be disseminated to a large audience very quickly, shaping public opinion and influencing societal norms and values. Mass media can influence the way people think and feel about certain issues, events, or people. By framing a story in a particular way, the media can shape public opinion about the issue, which can in turn influence policy decisions and public behavior. Mass media can also set the agenda by choosing which stories to cover and how much coverage to give to each story. This can influence what people think is important and what they should be paying attention to. Mass media has the power to bring attention to social issues, injustices, and other problems that might otherwise go unnoticed. By highlighting these issues, the media can create awareness and motivate people to take action.

Mass media can be a powerful tool for generating revenue through advertising and other forms of marketing. This can give media organizations significant influence over the products and services that people consume. We believe it would also be important to make a distinction between the mainstream and alternative media. The mainstream media refers to the large, established media outlets that are widely recognized and accepted as credible sources of news and information, such as major television networks, newspapers, and news websites. These outlets have significant resources, reach a large audience, and are often associated with a particular political or ideological perspective. Alternative media, on the other hand, refers to smaller, often independent media outlets that provide an alternative perspective to the mainstream. Alternative media outlets may be run by individuals or grassroots organizations, and often focus on issues that are not widely covered by the mainstream media. Alternative media may include blogs, podcasts, independent newspapers, and social media platforms. The

mainstream media is often funded through advertising revenue and subscriptions, while alternative media may rely on donations, crowdfunding, or other forms of grassroots support. The mainstream media is often associated with a particular political or ideological perspective, while alternative media may provide a more diverse range of perspectives and viewpoints.

Alternative or mainstream, the power of mass media lies in its ability to reach a large audience and shape public opinion. With this power comes responsibility, and it is important for media organizations to use their platform in a way that is ethical, unbiased, and in the best interest of society. Unfortunately, as media consumption has increased, a new kind of journalism emerged. The motivation behind this new exercise is not spreading information but increasing sales. 'Yellow Journalism' is a style of sensationalist and irresponsible reporting that emerged in the late 19th century in the United States. The term "yellow journalism" was coined by Erwin Wardman, the editor of the New York Press, in 1897, to describe the sensationalist and often exaggerated reporting of the era's newspapers[41].

The roots of yellow journalism can be traced back to the rivalry between two of the era's most influential newspaper publishers: Joseph Pulitzer, owner of the New York World, and William Randolph Hearst, owner of the New York Journal. The two men were in fierce competition to capture readership and increase circulation, and they employed a variety of sensationalist tactics to achieve their goals. Pulitzer and Hearst both used sensational headlines, lurid illustrations, and exaggerated stories to attract readers. They also employed several unethical practices, such as using fake interviews, staging events, and fabricating stories. They often relied on anonymous sources and hearsay, and frequently published unverified rumors and outright falsehoods. One of the most famous examples of yellow journalism was the coverage of the sinking of the USS Maine in Havana Harbor in 1898. Hearst's Journal and Pulitzer's World both ran stories that blamed Spain for the incident, despite the lack of evidence. The coverage helped to inflame public opinion and played a significant role in the outbreak of the Spanish-American War[42].

Yellow journalism eventually fell out of favor as the public became increasingly aware of the unethical practices used by publishers. However, its legacy can still be seen in modern tabloid journalism, which often relies on sensational headlines and

---

41 Campbell, W. J. (2001). Yellow journalism: Puncturing the myths, defining the legacies. Greenwood Publishing Group.

42 Biagi, S. (2014). Media/Impact: An introduction to mass media. Cengage Learning.

exaggerated stories to attract readership. Especially after the 9/11 attacks in the United States, terrorism became a frequently used topic to create such sensational news.

The representation of the subject of terrorism has become so problematic that these publications may even have somehow started to contribute to terrorism. Sensationalist journalism can contribute to the problem of terrorism in several ways: Terrorism is often carried out by groups or individuals seeking attention and recognition. Sensationalist journalism can provide the attention and coverage that terrorists seek, which can encourage further attacks. Sensationalist journalism often plays on people's fears and anxieties, which can exacerbate the perception of terrorism as a threat and contribute to a culture of fear. It may reinforce harmful stereotypes about certain groups or communities, such as Muslims or people of Middle Eastern descent, which can contribute to the rise of extremism and terrorism in the specified communities. Sensationalist journalism may simplify complex political, social, or economic issues that contribute to the rise of terrorism, which can lead to a lack of understanding of the root causes of terrorism and a failure to address them effectively. The coverage of terrorist attacks can also inspire copycat behavior and encourage others to carry out similar attacks to gain attention and recognition.

Representations of terrorism in the media and popular culture often perpetuate Islamophobic stereotypes and reinforce negative attitudes towards Muslims. Muslims are frequently depicted as terrorists or potential terrorists, and their religion is often portrayed as inherently violent and backward. These representations are not only inaccurate but also harmful, as they contribute to the stigmatization and marginalization of Muslim communities. They can also create a climate of fear and suspicion, which can lead to discrimination, hate crimes, and even violence against Muslims.

Furthermore, the link between Islamophobia and terrorism representations can also have broader geopolitical implications. It can reinforce a narrative of a "clash of civilizations" between the West and the Muslim world and contribute to the justification of military interventions and other forms of foreign policy that target Muslim-majority countries.

It is especially important to challenge Islamophobic representations of terrorism and to recognize the diversity and complexity of Muslim communities. This includes promoting accurate and nuanced portrayals of Islam and Muslims in the media and popular culture, as well as supporting efforts to combat discrimination and hate crimes against Muslims. Douglas Kellner states that after September 11 attacks both countries used media texts to propagate their agenda which Kellner defines as a

hegemonic political narrative[43]. The acts of political violence represented in the media after September 11 attacks presented these events as a clash of civilizations as using wordings such as: “good versus evil” and “us versus them”. In this way media ecosystem hardly represents events objectively. Research aimed at understanding these contradictions is still debated in contemporary academic circles.

Methodology

In this section the assassination of Japan’s Prime Minister Shinzo Abe will be examined as an act of political violence. Japan’s democracy was compromised by the event as in democratic societies freedom of speech is a major matter[44]. Using tools like Google News can provide a convenient way to access a wide range of articles for analysis in terms of covering the event by different news companies.

To examine the event, four news outlets from three different countries/cultures were chosen: The New York Times; the Los Angeles Times; the South China Morning Post; and the Straits Times. First we looked at the readership of these news outlets and concluded that most read digital news outlets are in U.S. The New York Times and Los Angeles Times[45]. The media companies were chosen from Western countries such as U.S., and East, including China and Singapore. Due to the time constraints of the research we looked two news companies form West and two news companies from East. (This can be identified as a limitation of the study.) The authors aim to find whether the east/west dichotomy exists in media. Through media framing methods and content analysis, the research questions will be explored. The research questions had been given below respectively:

R. Q. 1) Are there any differences between Western and Eastern media outlets in their portrayal of terror or acts of political violence?

Four publications from three countries were chosen because they have large readerships and have an impact on how news is covered in their respective nations. Comparative analysis of the media companies from different countries

---

43 Kellner, D. (2004). 9/11, spectacles of terror, and media manipulation: A critique of Jihadist and Bush media politics. Critical Discourse Studies, 1(1), 41-64.

44 The prime minister had been assassinated while giving a public speech which was a speech for a political campaign.

45 Altough there are different online news companies that have more reader, we excluded the websites that needs subscription. We experienced this issue generally about Western news companies. Furthermore several news companies from China do not have English translation on their website so again we had to exclude which uses only one language.

allows researchers to find different framing techniques used by media companies. A coding scheme was constituted for the research, and the criteria or keywords that had been looked at on digital news were presented on table 3. which are; Unification Church, Security, International Relations, Gun Law, Photograph, Liberal Democratic Party (LDP), Tetsuya Yamagami, Family, Past Scandals, Political Violence. The continents of the Americas in the east, Asia, and Oceania in the west represent the pacific and the media companies had been chosen according to it.

Table 1. Selected Newspapers for Research

U.S.	China	Singapore
The New York Times	South China Morning Post	Straits Times
Los Angeles Times		

Through the methodology of focus coding following topics are the most used words in the covering of the assassination: Unification Church, Security, International Relations, Gun Law, Photograph, Liberal Democratic Party (LDP), Tetsuya Yamagami, Family, Past Scandals, and Political Violence. In this way, several items of news coverage used sensationalist perspectives such as referencing Shinzo Abe's past scandals and ties with the Unification Church. Another significant perspective was about Japan's laws and political stance in the World such as; Security, International Relations of the nation, and gun law. Lastly, the killer's name, political violence, usage of the photograph, and Abe's family were notably referenced in the digital news articles. These can be interpreted as personal pieces of information about both Yamagami and Abe. From the framing of the events, three perspectives come out through the focus coding method.

Case Study: Assassination of Japan's Prime Minister Shinzo Abe

In the following section chosen newspapers and the framing of the news will be investigated through this context. To research the assassination of Prime Minister Shinzo Abe, western and Asian news companies were selected. To be able to determine the news that covered the assassination, the heading and the sub-heading of the news had been read by researchers. If those categorizations did not refer to the assassination, it had been not counted as news that covered the event. The data collection date range is limited to the year 2022 as the assassination

happened in that year. In this way, the obtained data is between 8 July 2022 and 31 December 2022 respectively. We looked at selected newspapers on Google News and searched for the articles that refer to assassination of Shinzo Abe.

Table 2. List of news that cover the event (chosen according to the heading and subheading on google news)

News Agency	Number of News
The New York Times	6
Los Angeles Times	14
South China Morning Post	44
Straits Times	15

In 2022 the news outlets referenced above covered Shinzo Abe's assassination more than once on their websites. The obtained data shows that the Chinese news agency South China Morning Post covered the event many times compared to the other news agencies. The news company that covered the story least times was the New York Times.

Close reading of the first published news from all companies presented a scheme for analyzing. Content Analysis of the news reporting demonstrates that the codes given below are the most used words while framing the event in digital media.

Table 3. Coding Scheme for Content Analysis

	The New York Times	Los Angeles Times	South China Morning Post	Straits Times
Unification Church				X
Security	X			
International Relations	X	X	X	X
Gun Law	X	X		
Photograph	X	X	X	X
Liberal Democratic Party (LDP)		X	X	X
Tetsuya Yamagami		X	X	
Family	X	X	X	X
Past Scandals				X
Political Violence	X			

The coding scheme for content analysis is categorized according to the framing of the news stories, as seen in Table 3. the covering of the assassination varied according to the news companies. Tetsuya Yamagami's statement of the event that points to the connection of Prime Minister Shinzo Abe to the Unification Church only appeared in Singapoure-based news company Straits Times. The assassination also attracted security-related issues however only Western media companies covered Japan's security issues concerning the event.

It was discovered that all of the news companies emphasized the international relationship of Japan to other countries such as; the United States and China. Furthermore, all of the digital news had some photographs relating to the assassination. Lastly, all of the news outlets covered the family history of Shinzo Abe.

The Western media covered the story more extensively compared to the Asian news companies and described the event as a political violence incident. In this way, Asian media framed the event more dramatically as including the past scandals of the Liberal Democratic Party (LDP) which Shinzo Abe is a member. In a way, Asian media used a more provocative and scandalous tone while reporting the assassination. In addition to this, only The New York Times covered the event as a political violence act.

Conclusion

Understanding the relationship between media and political violence requires a nuanced analysis of specific contexts, including the political, social, and cultural dynamics at play. Therefore, the definition of political violence and the portrayal of these events in the media is a complicated topic. Yet, the definition of terrorism and how it should be reported may vary depending on the media outlet. This contradiction might be caused, in part, by the absence of a generally acknowledged definition of terror framing by editors. The relationship between media and terrorism presented in the literature review supports these issues. As seen in literature, there are many different terrorism definitions, through the case study it has been shown that media also portrays terror events in different contexts. The article compared how different news sources frame the same events or issues. We looked for patterns, similarities, and differences in their approaches.

To explore these issues a political violence act and its representation in digital media had been chosen as a case study. According to the research question, the author used framing theory through the methodology of focus coding. In this way, cultural differences while framing of the assassination looked through the articles and several topics significantly distinct in terms of framing the event.

To represent Western companies, we looked at news from; The New York Times Los Angeles Times and to represent East; South China Morning Post, Straits Times. After collecting the data keywords have been put forward. It was seen that Asian companies used a more scandalous tone as opposed to Western news agencies. The keywords show that Asian media framed the event more dramatically. Furthermore; Western media companies defined the event as a political violence act and give more news on the topic on their website.

However, this article has several limitations in terms of gathering the data, in this way although there are differences on framing the political violence act by media companies; it is important to note that these distinctions are generalizations and may not apply universally. Through content analysis we believe that there are main topics used mutually but the representation differed. Because of the scope of the study we have not discussed government control and freedom of the press, cultural sensitivity, the influence of state on the news media, all of which are topics that impact significantly on the news coverage and the framing of acts of political violence. The article shows that, it is difficult to create a mutual understanding of terrorism both scholarly and in media. The coding scheme that have been created for the study shows that cultural differences and international relations have impact on framing news events.

Bibliography

Allen, C. (2010). Islamophobia. Ashgate Publishing.

Ashraf, A., & Foggett, S. Media and Counter-terrorism. COUNTER TERRORISM, 127.

Biagi, S. (2014). Media/Impact: An introduction to mass media. Cengage Learning.

Bosi, L., & Malthaner, S. (2015). Political violence. The Oxford handbook of social movements, 440-451.

Bronowski, J. (2011). The ascent of man. Random House.

Calhoun, C. (2012). Communication as a Social Science (and more). Intercom: Revista Brasileira de Ciências da Comunicação, 35, 277-310.

Campbell, W. J. (2001). Yellow journalism: Puncturing the myths, defining the legacies. Greenwood Publishing Group.

Coady, C. A. J. (2021). The meaning of terrorism. Oxford University Press.

Cohen, B. C. (2015). Press and foreign policy (Vol. 2321). Princeton university press.

Coleman, R., McCombs, M., Shaw, D., & Weaver, D. (2009). Agenda setting. In The handbook of journalism studies (pp. 167-180). Routledge.

Entman, R.M. 1993. "Framing: Towards Clarification of a Fractured Paradigm."Journal of Communication43(4):51–85

Erlenbusch, V. (2015). Terrorism and revolutionary violence: The emergence of terrorism in the French Revolution. Critical Studies on Terrorism, 8(2), 193-210.

Gerbner, G., Gross, L., Morgan, M., & Signorielli, N. (1986). Living with television: The dynamics of the cultivation process. Perspectives on media effects, 1986, 17-40.

Goffman, E. (1974). Frame Analysis Cambridge. Mass.: Harvard Univ.

Hobbes, T. (1967). Hobbes's leviathan. Рипол Классик.

Kellner, D. (2004). 9/11, spectacles of terror, and media manipulation: A critique of Jihadist and Bush media politics. Critical Discourse Studies, 1(1), 41-64.

Kellner, D. (2004). 9/11, spectacles of terror, and media manipulation: A critique of Jihadist and Bush media politics. Critical Discourse Studies, 1(1), 41-64.

Lippmann, W. (2017). Public opinion. Routledge.

McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. Public opinion quarterly, 36(2), 176-187.

Nabi, R. L., & Riddle, K. (2008). Personality traits, television viewing, and the cultivation effect. Journal of Broadcasting & Electronic Media, 52(3), 327-348.

Parker, T., & Sitter, N. (2016). The four horsemen of terrorism: It's not waves, it's strains. Terrorism and Political Violence, 28(2), 197-216.

Rapoport, D. C. (2019). The four waves of modern terrorism. In Transnational Terrorism (pp. 3-30). Routledge.

Ruigrok, N., & Van Atteveldt, W. (2007). Global angling with a local angle: How US, British, and Dutch newspapers frame global and local terrorist attacks. Harvard International Journal of Press/Politics, 12(1), 68-90.

Saunders, B. (2008). Acts of self-harming protest and the definition of terrorism.

Schmid, A. (2004). Terrorism-the definitional problem. Case W. Res. J. Int'l L., 36, 375.

Schmid, A. P. (2004). Frameworks for conceptualising terrorism. Terrorism and political violence, 16(2), 197-221.

Schmid, A. P. (2011). The definition of terrorism. In The Routledge handbook of terrorism research (pp. 39-157). Routledge.

Van Prooijen, J. W., & Kuijper, S. M. (2020). A comparison of extreme religious and political ideologies: Similar worldviews but different grievances. Personality and Individual Differences, 159, 109888.

Wanta, W., & Hu, Y. W. (1993). The agenda-setting effects of international news coverage: An examination of differing news frames. International Journal of Public Opinion Research, 5(3), 250-264.

Whitley, D. S. (2009). Cave paintings and the human spirit: The origin of creativity and belief. Prometheus Books.

PUBLISHING PRINCIPLES

Articles sent to the ***Defence Against Terrorism Review*** must not be published elsewhere or must not have been sent to another publication in order to be published. Once the articles are submitted to DATR, the authors must acknowledge that they cannot submit their articles to other publications unless the total rejection of concerned articles by the Editor or the Endorsement Committee (EC).

The authors who try to submit their already published (even electronically) articles to DATR will not be accepted to submit their articles again and will be forbidden to participate any future activity conducted by COE-DAT.

A. GENERAL PRINCIPLES

1. Language of publication is English. The texts submitted must be clear and understandable, and be in line with scientific/academic criteria in terms of language, expression and citation.

2. The texts submitted to be published must be between 4000 and 12000 words including the abstract and bibliography.

3. The texts must be submitted together with an abstract no longer than 300 words at the beginning of the paper and with five keywords after the abstract.

4. The name of the author must be placed in the first footnote, with his/her title, place of duty and e-mail address. Footnotes for other explanations must be provided both in the text and down the page in numbers.

5. The type character must be Arial, “11 type size”, line spacing “1,5 nk”, footnotes in “9 type size” and with “single” line spacing.

General Contents

The following are general stylistic conventions used by COE-DAT:

1. Writing must be scholarly in nature and not overly conversational. Do not use “I” or “we” but “the author” or the “authors.”

2. Do not use contractions except in quotes.

3. Except in quotes, do not underline or bold text to emphasize it but instead use word order for emphasis. To highlight a term, show the key words in single mark (‘aerospace’).

4. Use italic font for foreign phrases and names of court cases.

5. For dates, use – date month year format (10 March 2011) – not numbers (10/03/11). In footnotes, dates of the sources may follow the format used in the source.

6. There should be only one space between the period at the end of a sentence and the beginning of the next sentence.

7. Acronyms should be defined when first used with the full name in parentheses after the acronym; acronyms in foreign languages should have the name in the foreign first in parentheses, followed by the English translation. If an acronym has been defined once in the text of the article, it is unnecessary to spell it out again either in text or footnotes.

8. Numbers less than twenty or less should be spelled out; numbers 21 and above should be left in numbers.

9. Values in currency should be quoted in the actual currency followed by the amount in dollars (USD) or euros (€) in parentheses.

10. While making quotations;

a. If the part taken from the source is 4 lines and less than 4 lines, quotation marks ("... sentence...") can be used.

b. If the part taken from the source is more than 4 lines, it must be given with extra indentations.

- In addition, the writer of the article must avoid excessive use of each source, in particular from their own previous writings.

B. PRINCIPLES AS TO PAGE LAYOUT

Formatting: Double-spaced with standard page margins. The text and all headings should be left justified. Set language as American English. The publisher employed by COE-DAT uses a particular document formatting that will be applied by the editors.

C. PRINCIPLES AS TO REFERENCES AND CITATIONS

Citations shall be given down the pages in numbers in Defence Against Terrorism Review and Citations shall be given down the pages with Chicago style. shall not be presented in the text (e.g. Waltz, 2009: 101.).

Full identity of the resources cited shall be given; any resource not actually cite shall not be presented in the bibliography.

Format for footnote citations;

1. For Books

a. Books with Single Author:

Name and surname of the author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s). For example;

Joseph Needham, *Science and Civilization in China,* (Vol. 5, Cambridge Univ. Pres, 1954), p.7.

Joseph Needham, *Science in Traditional China* (Harvard Univ. Pres, 1981), p. 37.

b. Books with Two or Three Authors:

Name and surname of the first author, name and surname of the second author, name and surname of the third author, *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s). For instance;

Joseph S. Nye Jr. and David A. Welch, *Understanding Global Conflict and Cooperation*, (Pearson Publication, 2011), p. 280.

c. Books with More Than Three Authors:

Name and surname of the first author et. al., *name of work* ("volume no" if applicable, translator if any, publisher and date of publication), page number(s). For example;

Luis Benton et. al., *Informal Economy,* (The John Hopkins University Press, 1989), pp. 47-59.

d. Books with Name of Author or Editor Non-Specified:

Redefining Security (Praeger Publication, 1998), p. 81.

2. For Articles

Name and surname of the author (for all authors if two or three, if more than three authors just for the first author and et. al.), "name of the article" (translator if any), *name of periodical in which it is published*, volume number (issue) (publication year), pages in journal, cited page number.

a. Articles with One Author:

Barry Buzan, "New Patterns of Global Security in the Twenty-First Century," *International Affairs* 67(3) (1991), pp. 431-451, p. 442.

b. Articles in Compilation Books:

Barry Buzan, "Is International Security Possible?", in *New Thinking About Strategy and International Security* (Ken Botth and Don Kaufman, eds, Harper Collins, 1991), pp. 31-55, p. 42.

c. Articles from Daily Newspapers:

Yossi Melman, "Computer Virus in Iran Actually Targeted Larger Nuclear Facility", *Haaretz* (22 September 2011), p. 7.

"Tehran's nuclear ambitions", *The Washington Post* (26 September 2009), p. 5.

3. For Theses

No italics shall be used for the titles of non-published theses. Name and surname of the author, "title of the thesis" (whether it has been published and academic degree of the thesis, institution and institute of the thesis, date of the thesis), page number. For instance;

Atasay Özdemir, "Approaches of the Effective Actors of the International System to Iran's Nuclear Programme" (Unpublished Doctoral Thesis, War College Strategic Researchs Institute, Istanbul, 2013), p. 22.

4. For Reports

a. Report with Author Specified

Tariq Khaitous, "Arab Reactions to a Nuclear Armed Iran" (Washington Institute for Near East Policy, Policy Focus 94, June 2009), p. 14.

b. Report with Author Non-Specified

Albania Country Report (T‹KA Publishing, 1995), p. 7.

c. Report prepared by an Institution, Firm or Institute

American Petroleum Institute, "Drilling and Production Practice Proceedings of the Spring Meeting" (Shell Development Company, 1956), p. 42.

d. For Internet Resources

If any of the above resources are available on the Internet, follow the citation above with "available at" with the full http address and the date accessed in paratheses.

e. Web Pages

"The World Factbook-Turkey," Central Intelligence Agency, available at https://www.cia.gov/library/publications/the-world-factbook/geos/tr.htm (accessed 25 February 2013).

"Dimona: Negev Nuclear Research Center," *Global Security*, available at http://www.

globalsecurity.org/wmd/world/israel/dimona.htm (accessed 11 January 2010).

"Russia's National Security Strategy to 2020" (12 May 2009), *Rustrans*, available at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 (accessed 02 May 2011).

5. Subsequent citations of the same source:

a. If the citation is to the footnote directly before, use "Ibid" – if the page or paragraph changes, you can add the new information, as in "Ibid, p. 48" or "Ibid, para. 68".

b. If the source is earlier than the previous one, use the author's last name (if there is one), followed by the name of the article, followed by the new page or paragraphe number. For example;

Buzan, "Is International Security Possible?", p. 48.

D. PRINCIPLES TO ABIDE BY IN USING OF DOCUMENTS, TABLES, FIGURES AND GRAPHICS

1. Attachments (documents), shall be presented at the end of the text and down below shall be a brief information as to the content of the document and proper citation in line with the relevant criteria.

2. Other attachments (Table, Figure, and Graphics) shall be presented as Additional Table: 1, Additional Graphic: 3 and Additional Figure: 7. If indicators other than the text are too many in number; attachments shall be presented after the References.

a. References to these attachments in the text shall absolutely be made as Additional Table: 1, Additional Graphic: 3 or Additional Figure: 7.

b. If citation has been made for table, figure, graphic or picture, the source shall absolutely be indicated.

3. The names of the tables within the text shall be written on the top of the table and these tables shall be cited in the footnote according the publication type from which it was cited.

4. The names of the figures, graphics and maps within the text shall be written at the bottom of the figures, graphics and maps and these figures, graphics and maps shall be citied in the footnote according the publication type from which it was cited.

E. PRINCIPLES TO ABIDE BY IN BIBLIOGRAPHY

1. Just like giving citations but this time surname of the author shall be at the beginning.
2. Resources shall be sorted alphabetically from A to Z.
3. Page numbers shall not be indicated.

"Scan to reach the software of this publication and the other products of COE-DAT"

www.coedat.nato.int