Turkish Journal of Forensic Science and Crime Studies

ISSN: 2687-3397
Year: 6, **Volume:** 6, **Issue:** 1, March 2024 p. 3-21 **Article Type:** Review Article
Received Date: 24.02.2024 **Accepted Date:** 27.03.2024

Theoretical Approaches to The Psychology of Cyberterrorism

Nedim Havle[*], Sudiye Aksoy[**]

Abstract: Cyberterrorism is emerging as a complex and multidimensional threat to contemporary societies. This paper emphasizes that cyberterrorism is not only a technological phenomenon, but also a complex response to human psychology and social structures. It explores how individuals' experiences of social exclusion, identity crises, and perceptions of injustice have a critical impact on their participation in cyberterrorism. In this context, a comprehensive understanding of how cyberterrorism contributes to the radicalization process of individuals is necessary.

The article examines in detail the psychological dimensions of cyberterrorism, focusing on individuals' need for group affiliation, their deviation from social norms, and their adaptation to the radical ideologies of terrorism. The impact of cyberterrorism on society and its effects on human psychology are comprehensively assessed, as are the processes of radicalization. This analysis reveals the critical importance of understanding the psychological needs and social context of individuals, in addition to technological measures, in combating cyberterrorism.

The article argues that cyberterrorism should be treated as a complex phenomenon in which psychological, social, and technological factors interact. This multidisciplinary approach emphasizes the importance of the integrated use of psychological and sociological theories to understand and combat cyberterrorism. This approach proposes a holistic solution to better understand the impact of cyberterrorism on society and to effectively deal with this global threat.

Keywords: Cyberterrorism, Cybercrime, Human Psychology, Social Dynamics, Multidisciplinary Approach

[*] Psychiatry Specialist. T.C Ministry of Health Istanbul Bahçelievler State Hospital. nedimhavle@yahoo.com. ORCID No:0000-0003-2841-8460

[**] Instructor/Psychologist. T.C. Ministry of Justice Ord. Prof. Dr. Sulhi Dönmezer Education Center. sdyhsn@hotmail.com. ORCID No:0009-0002-1638-6887

Turkish Journal of Forensic Science and Crime Studies

ISSN: 2687-3397
Year: 6, **Volume:** 6, **Issue:** 1, March 2024 p. 3-21 **Article Type:** Review Article
Received Date: 24.02.2024 **Accepted Date:** 27.03.2024

Siber Terörizmin Psikolojisi Üzerine Kuramsal Yaklaşımlar

Nedim Havle[*], **Sudiye Aksoy**[**]

Özet: Günümüzün hızla dijitalleşen dünyasında, siber terörizm, toplumlar üzerinde derin ve çok yönlü etkiler yaratabilecek bir sorunsal olarak görülmektedir. Bu bağlamda sunulan çalışma, siber terörizmin teknolojik bir fenomenin ötesinde, bireyin psikolojisi ve sosyal yapılarla karmaşık bir şekilde etkileşim içinde olabileceğini önermektedir. Toplumsal dışlanma, kimlik bunalımları ve adaletsizlik algısı gibi bireysel deneyimlerin, siber terör eylemlerine katılımı nasıl şekillendirebileceği üzerinde durulmakta ve bu etkileşimler detaylı bir şekilde incelenmektedir. Siber terörizmin, bireylerin radikalleşme sürecine olan etkilerini anlamak bu çalışmanın temel amaçlarından biri olarak belirlenmiştir.

Makale, siber terörizmin psikolojik yönlerine dair ayrıntılı bir inceleme sunarken, bireylerin grup içi dinamiklere aidiyet duygusu, sosyal normlardan sapma eğilimleri ve radikal ideolojilere adaptasyon süreçlerinin üzerinde durmaktadır. Bu süreçler, toplum üzerindeki genel etkileri ve insan psikolojisi üzerindeki yansımaları ile birlikte, radikalleşme süreçleri ışığında incelenmektedir. Elde edilen bulgular, siber terörle mücadelede teknolojik önlemlerin yanı sıra, bireylerin psikolojik ihtiyaçlarını ve sosyal bağlamı dikkate alan bir yaklaşımın önemli olabileceğini öne sürmektedir.

Bu çalışma, siber terörizmin, psikolojik, sosyal ve teknolojik unsurların bir arada etkileşim içinde olabileceği karmaşık bir olgu olarak ele alınabileceğini savunmaktadır. Çok katmanlı bir sorunun çözümü için multidisipliner bir perspektifin önerilmesi, siber terörizme dair daha derin bir anlayışa ulaşılmasına ve bu küresel tehditle daha etkili bir mücadele stratejisi geliştirilmesine yardımcı olabilir. Psikolojik ve sosyolojik teorilerin entegrasyonunun önemi vurgulanırken, siber güvenlik politikalarının geliştirilmesinde bireylerin sosyo-psikolojik profillerinin ve toplumsal dinamiklerin göz önünde bulundurulması, siber terörizmin önlenmesi ve mücadele stratejilerinde yenilikçi yaklaşımlar geliştirilebileceği öne sürülmektedir. Bütüncül bir yaklaşımın benimsenmesi, siber terörizmin toplumsal etkilerinin daha iyi anlaşılmasına ve bu geniş çaplı tehditle daha etkin bir mücadele yöntemi geliştirilmesine olanak tanıyabilir.

Anahtar Kelimeler: Siber Terörizm, Siber Suç, İnsan Psikolojisi, Sosyal Dinamikler, Multidisipliner Yaklaşım

[*] Psikiyatri Uzmanı. T.C Sağlık Bakanlığı İstanbul Bahçelievler Devlet Hastanesi. nedimhavle@yahoo.com._ORCID No:0000-0003-2841-8460

[**] Öğretim Görevlisi/Psikolog. T.C. Adalet Bakanlığı Ord. Prof. Dr. Sulhi Dönmezer Eğitim Merkezi. sdyhsn@hotmail.com. ORCID No:0009-0002-1638-6887

Introduction

In the modern era of rapid technological advancement, cyber terrorism has become a threat that transcends traditional notions of security. The purpose of this article is to explore not only the technical and tactical dimensions of cyber terrorism, but also its psychological and sociological aspects. Our analysis will address the impact of cyberterrorism on the lives of individuals and societies, particularly in terms of psychological dynamics and social interactions. The paper examines the motivations underlying cyberterrorism and how they are intertwined with psychological factors such as individuals' perceptions of injustice, identity confusion, and the need to belong. It also discusses the impact of cyberterrorism on social structures and institutions in the context of ideological diffusion and group dynamics. Drawing on theories from cognitive and social psychology, this review examines how cyberterrorism affects individuals' behavior and thought processes. It examines the impact of cyberterrorism on individuals' moral decision-making processes, social identities, and group tendencies. Finally, it emphasizes the importance of multi-faceted strategies to counter cyberterrorism that go beyond purely technological measures and take into account psychological and sociological factors. This study will demonstrate the need for a holistic approach to understanding the complex nature of cyberterrorism and identifying effective ways to combat it.

Definition and Scope of Cybercrime

Cybercrime is one of the most prominent forms of crime in the digital age and is becoming increasingly complex as technology continues to evolve. This new type of crime goes beyond traditional concepts of crime and encompasses offenses committed with or against information technology. The definition and scope of cybercrime is critical to understanding and effectively combating it. Cybercrime is defined as illegal activities that typically take place over the Internet and target computers, networks, and digital data. These crimes can target the information and communication technologies of individuals, organizations, or governments. Cybercrime includes not only crimes committed using technological tools, but also cases where traditional crimes are committed using technology.

The scope of cybercrime is broad and varied and can be analyzed under the following headings:

Data breach and theft: This category includes the loss of personal information, financial data and trade secrets through unauthorized access or theft.

Identity theft and fraud: The theft of an individual's identity information and the use of that information to commit fraud or other illegal activities.

Software and hardware damage: The use of malicious software, such as viruses, Trojan horses and ransomware to damage or disable computer systems.

Cyber harassment and bullying: Actions taken over the Internet to threaten, harass, or harm individuals.

Intellectual property infringement: Violation of intellectual property rights, such as copyright, trademark or patent infringement.

State-sponsored cyberattacks: Attacks against the information systems of other states, organizations or individuals that are sponsored or carried out by states (Sabillon et al., 2016, pp. 165-176).

Most cybercrime is perpetrated by hackers. Hackers are individuals who seek out and exploit security vulnerabilities. They often have high intelligence, the ability to solve complex problems, and strong technical skills. Hackers can be divided into three main categories: White Hats, Black Hats, and Gray Hats. White hat hackers are ethical individuals who work to make systems more secure. Black hats engage in illegal activities, and cyber terrorists can also be included in this group. Grey hat hackers identify and publicize security vulnerabilities (Venue, 2012). The effects of cybercrime range from economic losses to social and psychological consequences. Financial losses, breaches of corporate and personal security, theft of personal information, and even threats to national security are among the damages that these crimes can cause.

Cyber Terrorism

Cyber terrorism can be defined as the process of meeting logistical needs through violent criminal acts, activities and propaganda carried out by members of terrorist organizations and associated individuals through network systems in order to achieve political goals. This definition includes acts carried out in cyberspace or using cyber tools that aim to create fear, cause harm, or disrupt public order (Vilic, 2017). Cyber terrorism has become one of the most important security challenges of the 21st century. With the advancement of technology and the spread of the Internet, this new form of terrorism poses a serious threat to international security, economic stability, and individual freedoms. Terrorist organizations prefer cyber attacks because they are less likely to be tracked, they can attack multiple targets, there is no risk of death, and they can act with an anonymous identity.

The scope of cyberterrorism can be analyzed under the following major headings:

Attacks on critical infrastructure: Cyber attacks on critical infrastructure such as power plants, water treatment facilities, transportation systems, and health care services.

Information systems damage: Cyber attacks on critical information systems such as government agencies, financial institutions, and large corporations.

Public opinion and propaganda: Manipulating public opinion and propaganda for terrorist organizations by spreading misleading information through social media and other online platforms.

Attacks on personal data: Gaining access to individuals' private information and using it for threats, blackmail, or other illegal purposes.

The effects of cyberterrorism are as follows:

Economic damage: Cyber attacks can disrupt the functioning of businesses and economic systems, causing massive financial losses.

Threats to security and stability: Attacks on critical infrastructure pose a serious threat to national security and social stability.

Political and social tensions: Misinformation and propaganda can increase political and social tensions and divide societies.

Privacy and security breaches: The theft and misuse of individuals' private information leads to privacy and security breaches (Sagiroglu & Arslan, 2019, pp. 239-244).

Cyberterrorism is a global threat that poses new and serious security challenges to states, organizations, and individuals in today's world. International cooperation, strong cybersecurity policies, and widespread public awareness are needed to properly understand, effectively prevent, and combat this threat (Broadhurst et al., 2017).

Theoretical Approaches

Cyberterrorism is a phenomenon that threatens not only national security, but also the psychological well-being of individuals and societies in the modern world. Unlike traditional terrorism, this form of digital threat takes place in a virtual environment but has deep and lasting effects in the real world. Cyberterrorism is typically driven by four main motivations: (1) opportunity to act, (2) need to belong, (3) desire for social status, and (4) financial gain. These motivations can be analyzed under three main themes: perception of injustice, identity confusion, and the problem of belonging (Shadach, Geller, Barak, Hill, & Azani, 2021), (Gross, Canetti, & Vashdi, 2016, pp. 284 - 291).

Perception of injustice

Cyberterrorist behavior is often based on a deeply rooted perception of injustice. This psychological underpinning plays a critical role in motivating individuals to engage in cyberterrorism. Perceptions of injustice typically focus on specific policies, individuals, governments, or entire nations and serve as a catalyst to legitimize aggressive behavior. Underlying these perceptions are cognitive biases that significantly distort an individual's view of reality. These distortions can lead to overgeneralizations and erroneous conclusions, and are often manifested in thought patterns such as "This is not right - This is not fair - This is your fault - You are the devil. Such thoughts not only justify aggression, but also reinforce a hostile image of the target. These perceptions are closely related to psychological defenses. Projection, for example, involves attributing one's own negative traits or emotions to others. In the context of cyberterrorism, this can mean projecting personal feelings of injustice onto the target person or group to further legitimize aggressive actions. Emotions such as anger and hostility are inextricably linked to perceptions of injustice and can provide a powerful psychological impetus for cyberterrorist activities. These intense emotions can drive individuals to commit acts of violence and aggression against specific social or political entities.

Furthermore, socio-economic status plays an important role in shaping these perceptions. Individuals from lower socioeconomic backgrounds may experience societal inequalities more acutely, as suggested by Polyakov and Starodubtseva (2019). This heightened sense of inequality may be a strong motivator for engaging in acts of cyberterrorism, as these individuals seek to address or avenge the injustices they perceive.

Revenge

The progression from perceived injustice to the desire for revenge is a central psychological trajectory in the context of cyberterrorism. This desire for revenge can manifest itself at both the individual and collective levels, often using cyberspace as a channel to retaliate against perceived wrongs to self or community. Central to this dynamic is the role of emotional responses, particularly anger and hostility, which are direct extensions of perceived injustices. The escalation of these emotions can significantly increase an individual's vengeful tendencies. Psychological frameworks emphasize the importance of emotional regulation in mitigating these intense vengeful desires.

From a psychiatric perspective, the desire for revenge can also be linked to narcissistic injuries and experiences of rejection. In the realm of cyberterrorism, individuals may resort to cyberattacks as a means of responding to personal slights. These actions are often motivated by the need to demonstrate power and maintain self-esteem, and may serve as a defense mechanism against perceived insult or humiliation. In addition, the collective dimension of revenge in cyberterrorism is also noteworthy. Individuals may respond not only to personal injustices, but also to perceived group injustices, and integrate these victimizations into their group identity. Cyberterrorism can reinforce this sense of collective identity, transforming individual revenge into a coordinated group effort.

Albert Bandura's theory of moral disengagement (Bandura, 1990, pp. 161-191) provides an important lens for understanding how acts of revenge can be morally rationalized. This theory can provide insight into how individuals find a justifiable framework for their vengeful actions by disengaging from established moral values and thus committing acts of cyberterrorism under the guise of revenge.

The desire for revenge in cyberterrorism is intricately tied to individuals' perceptions of injustice and the resulting emotional, social, and psychological processes. Understanding these processes is essential to a holistic understanding of the motivations that drive cyberterrorist activity. Identifying the roots of vengeful desires and effectively managing these emotions is important for developing strategies to prevent and counter acts of cyberterrorism.

Identity Confusion

The phenomenon of identity confusion plays a critical role in the psychological landscape of cyberterrorism. The development of a healthy and coherent personal identity is essential to the integrity and continuity of an individual's personality. In the absence of such development, individuals may find themselves drawn to extreme ideologies, including those espoused by terrorist groups. The concept of "identity mortgage," whereby an individual uncritically adopts a particular role, ideology, or identity, is particularly important in this context. The absolutist nature of extremist ideologies is often attractive to people struggling with the uncertainties and stressors of a complex and multifaceted world. Psychoanalytically, this predisposition can be linked to an incomplete superego structure, often resulting from the absence of a strong parental figure or guidance. Observations suggest that low parental authority and weak ego integrity are common traits among individuals who turn to cyberterrorist activities.

For individuals experiencing a fundamental gap in their sense of self, the lure of terrorist group membership may provide a semblance of identity and belonging. In these scenarios, group membership may become the dominant element of their psychosocial identity. This transformation often coincides with a process of "de-identification" in which the individual's sense of personal responsibility is diminished, setting the stage for increased antisocial or violent behavior. The unique environment of cyberspace exacerbates this confusion of identity. The ability to operate under pseudonyms and the perception of being untraceable feeds the sense of being "someone else" or "somewhere else. This distancing from one's true identity increases the influence of groupthink and reduces perceived personal responsibility for acts of violence, further entrenching individuals in the cyberterrorist mindset.

Understanding the intricacies of identity confusion and the resulting group dynamics is critical to addressing the psychological and psychiatric dimensions of individuals involved in cyberterrorism. Recognizing the role of identity in these processes is a critical step in developing effective policies and strategies against cyberterrorism.

The Problem of Belonging

The complex relationship between cyberterrorism and people's search for belonging, affiliation, and attachment requires a comprehensive social psychological examination. Central to this examination is the idea that the impulse to join terrorist organizations is often driven by a deep "need to belong," as demonstrated in research by Hogg, Hohman, and Rivera (2008, pp. 1269-1280). This need is particularly pronounced among those who feel marginalized and alienated from mainstream society.

From a social psychological perspective, belonging is recognized as a basic human need. Individuals struggling with social exclusion and alienation may be drawn to radical groups that promise to fill this void. By offering a surrogate "family" or community, these groups can provide an alternative to the sense of belonging that is often unattainable in the "real" world. However, this newfound sense of belonging can come at a significant personal cost. Membership in these groups can compel individuals to engage in behaviors that are diametrically opposed to their intrinsic moral and human values.

The dynamics of belonging in cyberterrorism are uniquely complex. The anonymity of digital space and the fungibility of online identities can create a different experience of belonging than traditional terrorist groups. Online environments can allow individuals to interact with extremist groups without the constraints of their real-world identities. This disconnect can accelerate the assimilation and acceptance of extremist ideologies.

Cyberterrorism thus becomes a particularly attractive avenue for those who feel disenfranchised and socially isolated. The sense of virtual belonging it provides can be a powerful catalyst, leading individuals to deviate from social norms and engage in actions that further the group's ideological goals. While this virtual community can alleviate feelings of alienation and social exclusion, it also sets the stage for a journey toward radicalization and acts of violence.

Ideology

The intersection of ideology and cyberterrorism can be understood in complex ways through a multidisciplinary lens that spans sociological and psychological paradigms. This complexity stems from how individuals acquire and internalize ideological beliefs, particularly in the digital environment.

Manuel Castells' theory of the "network society" (Castells, 2013, p. 26) provides a deep understanding of the structural role of the internet in the spread of radical ideologies. The specific design of the internet encourages the rapid dissemination of information, allowing extremist ideologies to reach a wider audience at an unprecedented speed. This digital architecture greatly increases the exposure of individuals to radical beliefs and facilitates the assimilation of these ideologies. Erik Erikson’s theory of identity development (Bishop, 2013, pp. 1055-1061) provides insight into the personal commitment to ideologies among cyberterrorists. In times of identity crisis, individuals often seek ideologies that provide a sense of belonging and purpose. In this context, cyberterrorism may become attractive by offering not only a clear identity, but also existential solutions and a sense of community. Leon Festinger’s theory of cognitive dissonance (Festinger, 1957) explores the psychological processes that drive individuals toward ideological conformity. Influenced by group dynamics and the desire for cognitive conformity, cyberterrorists may adopt increasingly radical ideologies. This conformity helps to minimize dissonance between personal beliefs and group actions, rationalizing and even valorizing acts of violence. Max Weber’s theories of authority (Weber, 2005) are helpful in understanding how cyberterrorist ideologies gain legitimacy. Charismatic or traditional authorities in these groups can often manipulate historical narratives or religious texts to legitimize violence and portray their actions as morally obligatory and imperative. Anthony Giddens’ (Giddens, 1999) structuration theory provides a broader social perspective by emphasizing how cyberterrorism affects social structures and institutions. Cyberterrorist activities exploit technological dependencies and vulnerabilities to achieve ideological goals. This process can lead to significant changes in security policy and public use of technology, revealing the pervasive influence of cyberterrorist ideology on societal dynamics.

In cyberterrorism, ideology can act as a catalyst for violence by providing a moral and political framework that shapes perceptions and guides actions. It attempts to link immediate behavior, such as violence, to long-term expectations or promised rewards. Making this connection often requires unwavering belief and acceptance, as the realization of these outcomes may be uncertain. The promise of significant outcomes or rewards acts as a powerful motivational force that reinforces adherence to the ideology.

Diffusion of Responsibility in Cyberterrorism

The concept of diffusion of responsibility in cyberterrorism can be critically analyzed through the lens of classic psychological studies and theories. Zimbardo’s Stanford Prison Experiment (Drury et al., 2012, pp. 161-170) and Milgram’s obedience experiments (Blass, 2009, pp. 37-45) provide important insights into how the collective dynamics of a group can influence the moral decisions of individuals. These studies show that, particularly in a group setting characterized by hierarchy or a strong authority figure, individuals often experience a dilution of personal responsibility that can lead to morally questionable actions.

In the realm of cyberterrorism, the anonymity afforded by online interactions and the physical distance of group members play an important role in reducing each member's sense of personal responsibility. This reduced sense of responsibility, coupled with the impersonal nature of digital interaction, can make it easier for individuals to act in accordance with group directives, even when these deviate from societal moral and ethical standards.

Anonymity further affects this dynamic by potentially eliminating the cognitive dissonance that individuals may experience regarding the consequences of their actions. In a state of anonymity, individuals may find it easier to engage in violent or harmful behavior because the separation from their real-world identities reduces the psychological discomfort typically associated with such actions.

Within cyberterrorist groups, there is often a strong identification of individual social identities with the collective identity of the group. This cohesion facilitates the distribution of responsibility among members and can encourage compliance with group norms and obedience to orders. This phenomenon is supported by the notion that group identity overrides individual identity and can result in a collective moral compass that may be very different from that of each individual member.

Erich Fromm's analysis of the mechanisms of adaptation and avoidance of authority (Fromm, 2017) is particularly relevant in this context. In cyberterrorism, individuals may suspend their personal moral and ethical judgments in favor of group directives. This suspension of individual morality may be exacerbated in cyberspace, where the physical isolation of members makes them more vulnerable to the influence of group norms and increases peer pressure.

The greater the pressure, the more likely individuals are to obey group commands, often without critical consideration of the moral consequences. This dynamic is particularly strong in cyberterrorist groups, where collective identity and goals can greatly overshadow individual ethical considerations.

Self, Identity, Anonymity

The complex interplay of self, identity, and anonymity in cyberterrorism can be examined through several theoretical lenses. Emile Durkheim's concept of anomie (Marks, 1974, pp. 329-363) provides a fundamental understanding of how the dissolution of social norms in the digital world leads to depersonalization. In cyberterrorism, this dissolution can create an uncertain space where social norms blur and personal identities lose their traditional foundations. This uncertainty can encourage disengagement from social structures, making individuals more vulnerable to the lure of cybercriminal activity.

Alfred Adler's theory of the inferiority complex (Enrique, Arranz, Zarza, 2021, pp.7-8) provides insight into the motivational underpinnings of cyber terrorists. Their behavior may stem from an internal need to overcome feelings of inadequacy. The virtual world provides an opportunity for these individuals to develop a sense of superiority and control that compensates for their real-life shortcomings. To further explore group dynamics, the phenomenon of group polarization (Navajas et al., 2019, p. 29) illustrates how online interactions can reinforce radical views. Cyberterrorist groups, in particular, can act as echo chambers where individuals are drawn to increasingly extreme ideologies. This polarization can exacerbate feelings of low self-esteem and division among group members. Anthony Giddens' concepts of modernity and identity applied to cyberspace (McNally & Wheale, 2020) suggest that technology facilitates the reconfiguration of the self. Individuals who engage in cyberterrorism often reconstruct their identities in the digital world, creating personas that are significantly different from their true selves. This dissonance makes cyberterrorism a more attractive prospect for those seeking to escape their perceived inadequacies. In this context, the role of anonymity is crucial. Based on Leon Festinger's theory of cognitive dissonance (Festinger, 1957), anonymity in cyberspace may allow individuals to more easily reconcile conflicting beliefs and behaviors. It may allow them to embrace radical ideologies without the burden of social norms and traditional moral constraints. Henri Tajfel's theory of social identity (Tajfel and Turner, 1979, pp. 33-47) further explains how group membership in cyberterrorist networks reinforces social identities. This process involves conforming to and internalizing group norms and values, often leading to the prioritization of group goals over individual ethics. Such dynamics can lead individuals to abandon moral constraints and resort to violence. Examining the concept of depersonalization (Vilanova et al., 2017), we find that anonymity in cyberterrorist groups can lead to a loss of individual identity, which is replaced by a collective group identity. This shift may make participation in harmful activities more psychologically acceptable by reducing individual moral responsibility. Erving Goffman's dramaturgical approach (Yüceer, 2018) sheds light on how individuals in cyberterrorist groups change their social interactions and self-presentations in online environments. The distinction between "backstage" (private) and "frontstage" (public) behavior becomes apparent, often leading to a sharp contrast between real identity and group persona. Anonymity can deepen this distinction by further aligning individual behavior with group norms.

Finally, Asch's concept of normative influence (Battal et al., 2018) illustrates the power of group pressure in the context of cyberterrorism. This pressure can influence individuals to adopt and practice radical ideologies. Anonymity can amplify this effect by removing barriers that might otherwise prevent radical behavioral change.

Obedience in Cyberterrorism

The concept of compliance in cyberterrorism can be complexly examined through Robert Cialdini's (Cialdini, 2006) theories of social influence, with a particular focus on the principles of conformity and social proof. These principles explain how individuals in online environments submit to the influence of authority figures or group pressure. In the realm of cyberterrorism, this can often manifest as individuals mirroring the behavior of other group members, which can significantly influence their moral reasoning.

Lawrence Kohlberg's work on moral development (Kohlberg, 1963, pp. 277-330) provides further insight into this phenomenon. In the context of cyberterrorism, the delegation of moral agency to an authority figure can significantly undermine an individual's capacity for moral decision-making. Kohlberg suggests that such a scenario can lead to a regression to lower levels of moral development, where ethical judgments are heavily influenced, if not dictated, by external authorities. Understanding the role of authority in cyberterrorism can be enriched by Max Weber's typology of authority (Weber, 2005), particularly the concept of charismatic authority. The influence of charismatic leaders in cyberspace can be profound. Such figures can significantly shape individuals' moral values and perceptions of personal responsibility, thereby increasing their willingness to engage in cyberterrorist activities. Philip Zimbardo's (Zimbardo, 2004) research on responsibility shifting is particularly relevant in this context. The anonymity inherent in cyberspace can lead to a reduced sense of personal responsibility, making moral deviance more likely. As a result, individuals in such environments may be more inclined to obey authority figures, often at the expense of their own moral decision-making processes. In addition, Irvin D. Yalom's theory of core factors in group therapy (Yalom, 2018) provides valuable insights into the dynamics within cyberterrorist groups. Factors such as group cohesion, shared beliefs, and common goals can reinforce submissive behavior among members. These dynamics can profoundly affect the moral reasoning of individual members, potentially leading them to commit acts of violence under the guise of group goals.

To better understand obedience in cyberterrorism, it may be useful to include case studies or real-world examples where these dynamics play an important role. Furthermore, exploring countermeasures or psychological interventions aimed at mitigating these effects could provide a balanced perspective on preventing radicalization in cyberspace.

Cognitive Reorganization

The process of moral disengagement in cyberterrorism can be effectively analyzed through the lens of cognitive psychology, with a particular focus on cognitive distortion mechanisms. These distortions skew individuals' perceptions of their actions and the resulting consequences, often significantly deviating from reality.

Drawing on Aaron Beck's theory of cognitive therapy (Beck, 1976), we see that individuals interpret their environment and themselves subjectively. This subjective perspective significantly influences moral value judgments and standards of behavior. In the context of cyberterrorism, this may mean that a cyberterrorist can rationalize his harmful actions by distorting the reality and effects of those actions. Henri Tajfel's social identity theory plays an important role in understanding the formation of group identities in cyberterrorism. As individuals embrace group membership and conform to group norms, there is a noticeable shift away from their personal identity. This shift can activate moral disengagement mechanisms, leading individuals to justify behavior that would otherwise be socially unacceptable. Leon Festinger's theory of cognitive dissonance provides insight into the ideological commitment of cyberterrorists. This theory argues that individuals naturally seek consistency in their beliefs and perceptions. In the case of cyber terrorists, this may often mean accepting information that is consistent with their ideological beliefs and rejecting contradictory evidence. Such selective perception and cognition may allow them to reframe destructive actions as consistent with ideological goals and further distance themselves from societal moral norms. Philip Zimbardo's concept of "deindividuation" (Zimbardo, 1969, pp. 237-307) is critical to understanding the impact of anonymity in cyberterrorism. Zimbardo argues that anonymity can significantly reduce moral constraints. In the realm of cyberterrorism, the combination of anonymity and remote interactions may reduce an individual's sense of responsibility, making moral detachment more likely.

Finally, Stanley Milgram's research on obedience highlights how authority figures can shape an individual's moral judgments. In cyberterrorist networks, leaders or ideological figures can exert significant influence, leading individuals to moral disengagement and encouraging actions that deviate from accepted societal norms. To deepen the understanding of cognitive restructuring in cyberterrorism, it would be useful to examine case studies where these psychological theories are brought to life. In addition, discussing potential interventions or training programs that address these cognitive biases could provide a more holistic perspective in combating cyberterrorism.

Moral Justification and Moral Reasoning

The concept of moral justification in cyberterrorism can be deeply understood through Albert Bandura's theory of moral disengagement. This theory posits that individuals sometimes deviate from their moral compass and use cognitive distortions to rationalize unacceptable behavior. In the realm of cyberterrorism, these distortions can be manipulated to legitimize attacks, often under the guise of political or social goals. This process can effectively blind individuals to the moral consequences of their actions, creating a dangerous disconnect between ethical standards and behavior.

Solomon Asch's seminal work on normative social influence (Asch, 1956, p. 1) further illuminates the powerful influence of group dynamics on individual moral reasoning. Within the confines of a cyberterrorist group, individuals may find themselves deviating from their personal moral beliefs under the influence of group norms and the directives of their leaders. This phenomenon illustrates how group pressure can significantly cloud an individual's moral judgment and lead to actions they would not consider on their own.

Cyberspace exacerbates this problem by reducing an individual's sense of responsibility. This digital dissociation facilitates the process of moral justification because the impersonal nature of cyberspace can make the consequences of one's actions feel less urgent or real. Lawrence Kohlberg's work on moral development provides further insight into how individuals in these groups may arrive at moral judgments. In the context of cyberterrorism, it seems plausible that an individual's morality may lean toward egoism or hedonism, placing immediate self-interest above established moral values. This perspective is often found in justifications for cyberattacks. In addition, the delayed moral reasoning of cyberterrorists may be related to deficiencies in their ethical decision-making processes. The unique dissociation provided by the Internet may lead individuals to ignore the real-world consequences of their actions, thereby compromising their ethical reasoning.

To strengthen this analysis, it may be instructive to include case studies of cyberterrorism incidents in which moral disengagement and group dynamics play a critical role. In addition, exploring strategies to improve ethical decision-making in digital environments may provide valuable insights into the moral justifications often used in cyberterrorism.

Victim blaming and disempowerment

The insidious strategy of victim blaming in cyberterrorism is based on Albert Bandura's theory of how attackers mentally legitimize their actions. This psychological maneuver involves a dangerous distortion of the victim's actions or character and can allow attackers to portray their attacks as not only legitimate, but necessary. This distorted logic can mitigate moral dissonance by transforming victims into instigators in the eyes of perpetrators. Extending this, research on social identity theory in the context of intergroup conflict provides insight into the construction of an enemy image. It shows how this distorted image significantly distorts individuals' moral judgments. Cyberterrorists use this tactic effectively; by dehumanizing their victims and stigmatizing them as inherently "bad" or "harmful," they can create a narrative that justifies their belligerent actions.

The neutralization theory of David Matza and Gresham Sykes (1957, pp. 664-670) further explains this phenomenon. It explains how cyber terrorists rationalize their behavior and numb their sense of moral responsibility. These techniques not only reduce the perpetrator's sense of guilt, but can also facilitate deviation from socially accepted moral norms. Philip Zimbardo's observations are particularly relevant in the context of cyberspace. He notes that anonymous environments such as the Internet significantly reduce the barriers to moral and ethical deviation. The anonymity and disconnectedness inherent in cyberspace can reduce one's sense of responsibility for one's actions. This environment is fertile ground for victim blaming and neutralization strategies, as it facilitates distancing from the real-world consequences of one's actions.

To gain a fuller understanding, one can examine real-world examples of cyberterrorism where victim blaming and disempowerment are prominent. In addition, discussing measures to counter these psychological tactics in cyber environments will provide a more balanced perspective and suggest ways to empower victims and hold perpetrators accountable.

Dehumanized victims

The phenomenon of dehumanization in cyberterrorism can be closely linked to Henri Tajfel's theory of social identity. In the dark corners of cyber conflict, the line between "us" and "them" can be blurred with alarming clarity. Emboldened by digital anonymity, cyberterrorists often place their adversaries in the "them" category and may perceive them not only as adversaries, but as subhuman or even transhuman beings. This alarming perspective is crucial to understanding the ease with which cyberterrorists deviate from moral norms and justify heinous acts against their perceived enemies. A closer examination of this process reveals how the usual empathic responses to humans are alarmingly blunted in the digital realm. The typical face-to-face interactions that humanize enemies are absent in cyberspace and can make the enemy an abstract concept rather than a real person. This disconnect plays a key role in making violence a more acceptable option for the cyberterrorist.

Albert Bandura's insights into the psychological underpinnings of "othering" enemies are particularly relevant here. Through a process of cognitive distortion fueled by group ideologies and prejudices, cyberterrorists are able to mentally justify their harmful actions. By dehumanizing their enemies, they see their actions not as crimes against humanity, but as necessary steps toward a perceived greater good. Case studies such as cyber attacks organized by ideologically motivated groups illustrate this dehumanization. For example, targeted attacks against specific ethnic or political groups, where the victims are reduced to symbols of a hated ideology [real-world case study if available], exemplify this phenomenon.

This dehumanization process is exacerbated by the pressures and ideological orientation within cyberterrorist groups. Within these groups, there is a collective mindset that legitimizes any action, no matter how violent, as long as it is in line with the group's goals. This collective mindset, explained by Bandura's social learning theory, can show how cyber terrorists learn and adopt these dehumanizing behaviors. Ideological diffusion within the group and the echo chamber effect of digital communication reinforce and normalize these attitudes. But this is not a one-way street. The psychological impact of this dehumanization on victims is profound. Victims can often suffer long-lasting psychological trauma as they are not only attacked, but also stripped of their humanity and identity in the eyes of their attackers. Society's response to these victims is often painted with the same dehumanizing brush, leading to further marginalization.

Addressing this dark side of cyberterrorism requires a multifaceted approach. Educational programs that foster digital empathy, policies that regulate online behavior, and strategies that promote positive group ideologies in cyberspace are particularly important. Understanding the unique mechanics of dehumanization in cyberterrorism compared to traditional terrorism can provide a pathway for developing targeted countermeasures. By addressing the underlying psychological processes that fuel this dehumanization, we can begin to reduce the power of cyberterrorists to dehumanize their victims.

Conclusion

This article has explored the complex landscape of cyberterrorism, demonstrating its multifaceted nature and significant consequences. Throughout the discourse, the idea that cyberterrorism transcends purely technological boundaries and encompasses deep psychological and sociological dimensions has been emphasized. This review argues for a broader perspective that goes beyond technological tools in combating cyber threats to include the psychological needs and social frameworks that surround individuals. The findings of this study underscore the need for comprehensive and integrative strategies to combat cyberterrorism. Complementing technological interventions with a nuanced understanding of the psychological impact of cyberterrorism and its embeddedness in social dynamics envisions a more nuanced and effective response to this pervasive threat. By placing the human element at the center of cybersecurity policy formulation, this approach is dedicated to developing societies that are not only resilient, but also deeply aware.

This paper aims to contribute to a nuanced understanding of the complex nature of cyberterrorism and the formulation of robust countermeasures. We believe that future research in this area has the potential to advance a holistic security paradigm that harmonizes technological and human-centered solutions. By effectively emphasizing interdisciplinary exchange in this concluding chapter, the scholarly contribution of this study is emphasized, thus infusing the literature with the richness of a multidisciplinary approach. This paves the way for innovative and comprehensive strategies to combat cyberterrorism. By shedding light on both the technological and human aspects of cyberterrorism, this study aims to enrich the body of knowledge in the field and guide future research. It is hoped that such efforts will play an important role in creating more informed and comprehensive policies against cyber terrorism.

References

Andik Matulessy, Nabilla H. Humaira. (2017). Hacker personality profiles reviewed in terms of the big five personality traits. Psychology and Behavior, 5(6), 137-142. https://doi.org/10.11648/j.pbs.20160506.12

Asch, S. E. (1956). Studies in independence and conformity: I. A minority of one against a unanimous majority. Psychological Monographs: General and Applied, 70(9), p.1

Bandura, A. (1990) ‘Moral Disengagement Mechanisms’, in W. Reich (ed.), The Origins of Terrorism: Psychologies, Ideologies, Theologies, Theologies, States of Mind (New York: Cambridge University Press, pp. 161-191,

Battal, F. Yıldız, Ş., Kılıçaslan, Ş., & Çınar, E. (2018). The relationship between the Solomon ash compatibility experiment and individuals’ decision-making styles (the case of Turkey).

Beck AT. (1976). Cognitive therapy and the emotional disorders. International Universities Press, New York,

Bishop,C.(2013).Psychosocial stages of development. pp.1055-1061. https://doi.org/10.1002/9781118339893.WBECCP441

Blass, T. (2009). From New Haven to Santa Clara: A historical perspective on the Milgram obedience experiments. The American Psychologist, 64 1, pp. 37-45. https://doi.org/10.1037/a0014434.

Broadhurst, Roderic, (2021). Cybercrime: Thieves, Swindlers, Bandits and Privateers in Cyberspace Broadhurst Roderic, ‘Cybercrime: thieves, swindlers, bandits and privateers in cyberspace’, in Cornish, Paul, ed. Handbook of Cybersecurity, Oxford University Press, forthcoming 2021., Available at SSRN: https://ssrn.com/abstract=3009574 or http://dx.doi.org/10.2139/ssrn.3009574)

Broadhurst, R., Woodford-Smith, H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt, B., & Alazab, M. (2017). Cyberterrorism: A research review: Australian National University Cybercrime Observatory research report for the Korean Institute of Criminology. . https://doi.org/10.2139/SSRN.2984101.)

Cialdini, R. (2006). The Psychology of Persuasion. Harper Collins e-books.

Drury, S., Hutchens, S., Shuttlesworth, D., & White, C. (2012). Philip G. Zimbardo on his career and the 40th anniversary of the Stanford Prison Experiment. History of Psychology, 15, pp.161-170. https://doi.org/10.1037/A0025884.

Enrique B. Arranz-Freijo & Florencia Barreto-Zarza (2021) The contributions of Alfred Adler (1870-1937) to the understanding of early childhood development, Early Child Development and Care, 191:p.7-8, 1133-1143, DOI: 10.1080/03004430.2020.1851215

Erich Fromm (2017), Escape from Freedom, Say Publications.

Felipe Vilanova, Francielle Machado Beria, Ângelo Brandelli Costa & Silvia Helena Koller | Justin Hackett (Reviewing Editor) (2017) Deindividuation: From Le Bon to the social identity model of deindividuation effects, Cogent Psychology, 4:1, DOI: 10.1080/23311908.2017.1308104

Festinger, L. (1957). A theory of cognitive dissonance. Stanford, California: Stanford University Press

Giddens, A. (1999). The Construction of Society: The Main Lines of the Theory of Structuring. (Translated by H. Özel). Ankara: Bilim ve Sanat Yayınları.

Gross, M., Canetti, D., & Vashdi, D. (2016). The psychological impact of cyberterrorism. Bulletin of the Atomic Scientists, 72, pp.284 - 291. https://doi.org/10.1080/00963402.2016.1216502.

Hogg, M., Hohman, Z., & Rivera, J. (2008). Why do people join groups? Three motivational accounts from social psychology. Social and Personality Psychology Compass, 2, pp.1269-1280. https://doi.org/10.1111/J.1751-9004.2008.00099.X.

Kohlberg, Lawrence (1963). "Moral Development and Identification," Child Psychology, The Sixty-second Yearbook of the National Society for the Study of Education (ed. H. W. Stevenson), Chicago, pp. 277-330.

Manuel Castells (2013) "The Rise of the Network Society", (3rd edition), Istanbul Bilgi University Publications, Istanbul, p.26.

Marks, S. (1974). Durkheim's theory of anomie. American Journal of Sociology, 80, pp.329 - 363. https://doi.org/10.1086/225803,

McNally, R. & Wheale, P. (2020). Biopatenting and Innovation: Contemporary Nomads and a New Global Order. Nature, Risk and Responsibility. https://doi.org/10.1007/978-1-349-27241-9_11.

Navajas, J., Heduan, F., Garrido, J., González, P., Garbulsky, G., Ariely, D., & Sigman, M. (2019). Reaching consensus in polarized moral debates. Current Biology, p. 29, 4124-4129.e6. https://doi.org/10.1016/j.cub.2019.10.018.

Polyakov, V. & Starodubtseva, M. (2019). Factors influencing motivation for terrorist activities being implemented with the use of information technologies in transboundary regions. Proceedings of the International Conference on Sustainable Development of Cross-Border Regions: Economic, Social and Security Challenges (ICSDCBR 2019). https://doi.org/10.2991/icsdcbr-19.2019.40.

Sabillon, Regner & Cano M., Jeimy & Serra-Ruiz, Jordi & Cavaller, Víctor. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security. 4. 165-176..

Shadach, E., Geller, S., Barak, M., Hill, I., & Azani, E. (2021). A psychological typology of terror organizations. Aggression and Violent Behavior, 58, 101562. https://doi.org/10.1016/J.AVB.2021.101562.

Sykes, Gresham M. - Matza, David (1957), "Techniques of Neutralization: A Theory of Delinquency", American Sociological Review, Vol.22, No: 6, pp. 664-670,

Ş.Sağıroğlu and B.Arslan (2019), "Fighting with Cyber Terror and Terrorism: Threats and Precautions," in Fighting with Cyber Terror and Terrorism: Threats and Precautions," 4th International Conference on Computer Science and Engineering, UBMK 2019,Samsun, Turkey, pp.239-244)

Tajfel H. and Turner, J. C. (1979). An Integrative Theory of Intergroup Conflict. In The Social Psychology of Intergroup Relations, pp.33-47. Brooks-Cole: California,

Venue, C.. (2012) A guide to computer hacking including vulnerabilities, hacking tools, cybercrime, hacker ethics such as White Hat, Black Hat, Grey Hat, and more. [United States]: [Webster's Digital Services].

Vilic Vida (2017). Dark Web, Cyber Terrorism And Cyber Warfare: Dark Side Of The Cyberspace.

Weber, M. (2005). Bureaucracy and Authority. (trans. H. B. Akın). Ankara: Address Publications.

Yalom Irvin D. (2018) Group Psychotherapy Theory and Practice. Pegasus Publications. Translator: Prof. Dr. Ataman Tangör, Uzm. Dr. Özgür Karaçam.

Yüceer, Y. E. (2018). Erving Goffman & Dramaturgy in the context of cinema and social interaction (Master's thesis, Pamukkale University Institute of Social Sciences).

Zimbardo, Philip G. (1969). "The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos", Nebraska Symposium on Motivation, 17, p. 237-307.

Zimbardo, Philip G. (2004). "A Situationist Perspective on the Psychology of Evil: Understanding How Good People Are Transformed into Perpetrators",The Social Psychology of Good and Evil, Ed. Arthur G. Miller, New York, London, , pp.21-50.