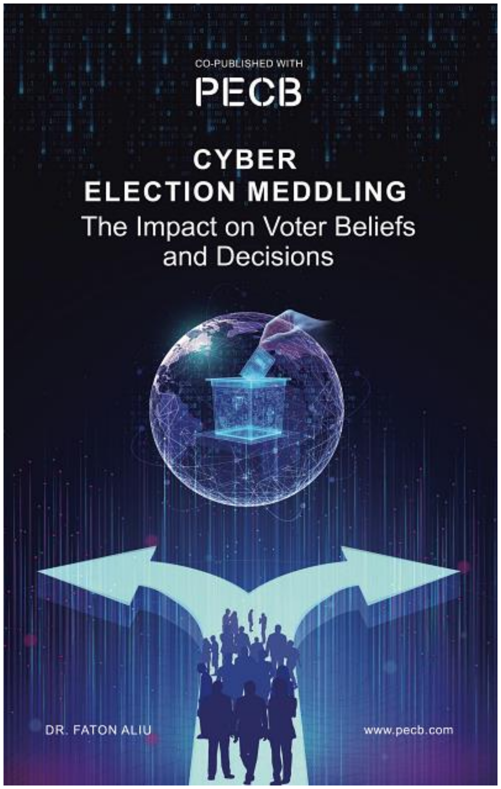


This research explores the effects of cyber election meddling on voter beliefs and decision making. It examines tactics, media influence, and implications for democratic integrity, providing insights into cybersecurity's role in elections.

Cyber Election Meddling:
The Impact on Voter Beliefs and Decisions

By Dr. Faton Aliu

CO-PUBLISHED WITH

PECB

CYBER ELECTION MEDDLING

The Impact on Voter Beliefs and Decisions

DR. FATON ALIU

www.pecb.com

Print ISBN: 978-1-959621-57-7
Ebook ISBN: 979-8-88531-878-5

Published by BookLocker.com, Inc., Trenton, Georgia.

BookLocker.com, Inc.
2024

First Edition

Library of Congress Cataloging in Publication Data
Aliu, Dr. Faton
Cyber Election Meddling: The Impact on Voter Beliefs and Decisions by Dr. Faton Aliu
Library of Congress Control Number: 2024923106

DISCLAIMER

This book details the author's personal research and opinions regarding cyber-election meddling and its impact on voter beliefs and decision-making. The author is not a licensed political scientist or attorney.

The author and publisher are providing this book and its contents on an “as is” basis and make no representations or warranties of any kind with respect to this book or its contents. The author and publisher disclaim all such representations and warranties, including, for example, warranties of merchantability and suitability for any particular purpose. In addition, the author and publisher do not represent or warrant that the information accessible via this book is accurate, complete, or current.

The statements made about policies, technology, and election systems have not been evaluated by any government agency. Please consult your legal, cybersecurity, or political expert regarding the implications and recommendations made in this book.

Except as expressly stated in this book, neither the author nor publisher nor any contributors or representatives will be liable for damages arising out of or in connection with the use of this book. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect, or consequential damages; loss of data, income, or profit; loss of or property damage; and claims of third parties.

You understand this book is not a substitute for consultation with licensed political, legal, or cybersecurity professionals. Before making any decisions or changes based on the content of this book, you should consult a licensed professional to ensure the best outcome for your situation.

This book is based on a doctoral study that takes a quantitative, non-experimental approach to examining the relationship between voters' belief in foreign election meddling and how it influences their decision-making process. Using the social cognitive theory as its framework, the research highlights the role of information sources in shaping voter perceptions, finding that those who relied on traditional news media rather than blogs or social media were more likely to recognize interference efforts. Use of this book implies your acceptance of this disclaimer.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

One critical feature of a democratic country is the conduct of free elections at regular intervals as prescribed by the country's constitution. In recent decades, it has become increasingly common for some countries to engage in interference with foreign elections (Tomz & Weeks, 2020). Research conducted by the Centre for the Study of Democratic Institutions at the University of British Columbia has identified four principal techniques used by foreign actors to interfere in elections: (a) hacking attacks targeting systems, accounts, and databases to access, alter, or leak private information; (b) mass misinformation and propaganda campaigns that promote false, deceptive, biased, and inflammatory messages, often utilizing bots or fake social media accounts; (c) acquisition of data on populations or individuals to develop messages for micro-targeted manipulation; and (d) conducting online "trolling" operations to threaten, stigmatize, and harass individuals or groups (Tenove et al., 2018). While not all foreign actors may utilize these techniques to interfere with elections, the deployment of even one can significantly influence election outcomes (Baines & Jones, 2018; Schmitt, 2021). The U.S. Senate Select Committee on Intelligence (SSCI) undertook a bipartisan investigation into various Russian activities connected to the 2016 U.S. presidential election (Burr et al., 2018). The Committee completed a comprehensive examination of the Intelligence Community Assessment (ICA) issued by the Central

Intelligence Agency (CIA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) in January 2017 concerning Russian interference in the 2016 U.S. presidential election (Office of the Director of National Intelligence, 2017). Addressing the issue of Russian cyber-interference in the election, the former Acting Director of the Central Intelligence Agency, Michael Morell, remarked, "It is an attack on our very democracy. It is an attack on who we are as a people… this is to me not an overstatement; this is the political equivalent of 9/11" (Morell & Kelly, 2016). Numerous reports have suggested that the Russian State Intelligence Agency might have illegally accessed the Democratic National Committee's internal servers and collaborated with WikiLeaks to release a collection of internal emails on the eve of the Democratic convention (Fidler, 2016). The NSA, CIA, and the FBI compiled a joint report detailing Moscow's employment of cyber activities aimed at undermining the democracy of the United States, a move seen as predictable due to the prolonged Cold War history between the two nations (Office of the Director of National Intelligence, 2017). The report contains sections that evoke Cold War sentiments, highlighting Moscow's intent to weaken the US-led liberal democratic order. However, the report distinguishes the efforts in 2016 by noting a significant escalation in Russia's direct influence efforts and an expansion in the level and scope of its activities beyond those of past operations (Office of the Director of National Intelligence, 2017). With high confidence, the report also acknowledges the Russian government's execution of a sophisticated social media campaign aimed at influencing the 2016 elections. Reflecting on the intensified efforts to exert influence, Russian Prime Minister Dmitry Medvedev commented at a security conference in Munich, Germany, "Sometimes I wonder if it is the year 2016 or 1962" (Hjelmgaard, 2016).

A 2017 memorandum by the Federal Election Commission (FEC) highlighted the American public's alarm at widespread reports of foreign influence on the 2016 presidential election, leading to an expectation of federal government action in response to the security breach (Vigdor, 2019). Former U.S. Vice President Dick Cheney suggested that Russia's alleged interference could be viewed as an "act of war" (Cahill, 2017). Additionally, investigations into Russian interference extended beyond the U.S., with the UK Electoral Commission, the UK Parliament's Culture Select Committee, and the U.S. Senate examining alleged Russian meddling in the "Brexit" referendum of June 23, 2016 (Intelligence and Security Committee of Parliament, 2020). The "Russia Report," a comprehensive 55-page analysis of Russia's malign interference in UK politics, was crafted by an independent committee comprising nine Members of Parliament from various political parties, including the ruling Conservatives. This report outlined the UK's significant underestimation of the threat posed by Russian interference and the government's subsequent struggles to address this issue effectively, leading to attempts by the Johnson administration to delay its release (Ellehuus & Ruy, 2020). Although some may argue that the disinformation and influence campaigns surrounding Brexit were somewhat limited in scope, the presence of Russian influence within UK politics is expected to persist as Russia continues its cyber-meddling efforts (Intelligence and

Security Committee of Parliament, 2020). This pattern of behavior, similar to Russia's interference in the 2016 U.S. presidential elections, suggests a broader trend of manipulation that is likely to continue (Schia & Gjesvik, 2020). The report delineates that if Russia played a role in influencing the 2016 Brexit referendum, it was not via direct meddling in the voting process, which in the United Kingdom is conducted exclusively with paper ballots and is considered highly secure. Instead, the report points to the possibility that Moscow-based misinformation campaigns disseminated through social media platforms and Russian state-funded broadcasters like Sputnik and RT could have played a significant role in shaping public opinion (Ellehuus & Ruy, 2020). This strategy, along with the recruitment of influential public figures to echo certain narratives, akin to tactics observed during the 2016 U.S. presidential election, contributed to the creation of a potent alternative narrative (Ellehuus & Ruy, 2020; Grinberg et al., 2019; Schia & Gjesvik, 2020). The controversy known as the Macron Leaks, which involved the leak of over 20,000 emails associated with Macron's campaign in the days leading up to his victory in the 2017 election, represents another instance of election meddling (Downing & Ahmed, 2019). The 2017 French presidential election is notable not only for this leak of substantial amounts of hacked data on the eve of the vote, attributed to external efforts to influence the election outcome but also for highlighting the growing concern over the role of fake news in shaping electoral outcomes in democracies globally (Vilmer & Conley, 2018; Downing & Ahmed, 2019). In these cases, social media played a pivotal role in disseminating misinformation, underscoring its significant impact on public perception and democratic processes (Allcott & Gentzkow, 2017; Allcott et al., 2019; Downing & Ahmed, 2019; Ellehuus & Ruy, 2020; Wu et al., 2019).

Statement of the Problem

This research will address the specific problem that some voters lack an understanding of the relationship between their belief in cyber election meddling by foreign governments and its impact on their decision-making process in government elections (Baines & Jones, 2018; Sander, 2019). Ever since allegations of Russian meddling in the 2016 U.S. presidential election, cyber-influence operations have garnered worldwide attention. (Sander, 2019). The manipulation of voter perceptions is a major challenge to the legitimacy of elections (Wu et al., 2022). Following reports indicating the possibility of foreign cyber-meddling in the 2016 U.S. elections, voter perceptions may have been manipulated (Fidler, 2016). For example, the Internet Research Agency, LLC (IRA), a Russian organization funded by Yevgeniy Viktorovich Prigozhin, conducted social media operations targeted at large U.S. audiences to sow discord in the U.S. political system (Mueller, 2019a).

Furthermore, an investigation by the UK Electoral Commission, the UK Parliament's Culture Select Committee, alleged Russian interference in the "Brexit" poll of June 23, 2016 (Intelligence and Security Committee of Parliament, 2020). In particular, the report opens the possibility that Moscow-based information operations may have been a significant factor (Ellehuus & Ruy, 2020). Moreover, understanding how social media platforms impact public life is difficult (Bradshaw & Howard, 2018), and in some jurisdictions, spreading computational propaganda may be illegal (Howard et al., 2018). However, there is evidence that the strategies and techniques used by government cyber-troops have an impact and that their activities violate the norms of democratic practice (Howard et al., 2019).

Purpose of the Study

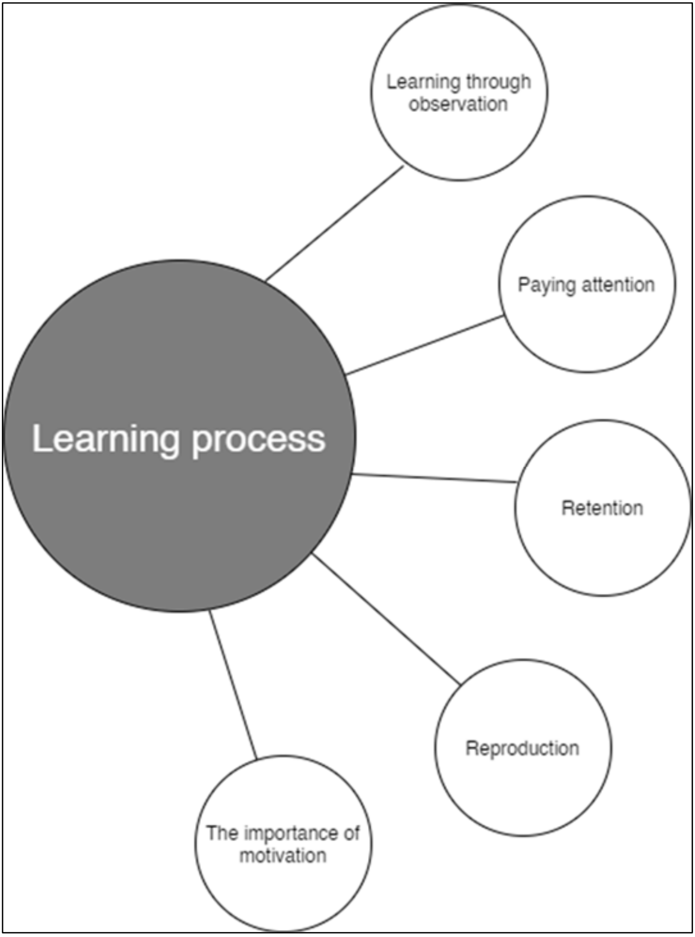
The purpose of this quantitative, non-experimental, cross-sectional, and correlational study was to provide an understanding of the relationship between voters' belief in cyber election meddling by foreign governments and their belief in its impact on their decision-making process in government elections. The population consisted of individuals who had voted in a national election since 2016. A minimum sample size of 115 participants was calculated using G*Power. The sample size calculation is based on an a priori power analysis for exact correlation, with correlation (p H1) of 0.30, $\alpha = 0.05$, and power of 95%. An online questionnaire was developed based on existing literature for data collection purposes and was validated through an initial pilot study. An invitation to participate was sent through LinkedIn’s direct messaging system. Participation was voluntary and anonymous. The variables in this study included (a) voter perception of cyber election meddling by foreign governments and (b) voters’ belief in its impact on their decision-making process. SPSS software version 28 was used to process the data and conduct the statistical analysis. Descriptive and inferential statistics were used to address the hypotheses and research questions of the study.

Theoretical Framework

The social cognitive theory (SCT) serves as the theoretical framework for this study. This theory posits that individuals learn and develop by observing others, acquiring information and skills through observation, and imitating others' behavior (Bandura & Walters, 1977). SCT emphasizes the role of social and environmental factors in shaping an individual's behavior and highlights the reciprocal relationship between cognitive, behavioral, and environmental variables (Bandura, 1986). This theory was deemed appropriate for this study as it sheds light on how individuals form attitudes and beliefs through observing and interpreting information from their social and physical environment. SCT suggests that attitudes and beliefs are shaped by direct personal experiences, as well as by indirect experiences, such as exposure to media, public opinion, and public discourse (Bandura, 1977), making it ideal for evaluating the reasons behind the voters' lack of understanding of how cyber election meddling by foreign governments may impact their voter decision-making process in government elections.

This study will examine the relationship between cyber-election meddling by foreign governments and their impact on the voter decision-making process in government elections. SCT provides a valuable framework for understanding how information from online sources can influence voter attitudes and beliefs and how these attitudes and beliefs can influence their vote and perception of the election outcomes. In particular, the theory suggests that the learning process includes several important factors, like (a) learning through observation, (b) paying attention, (c) retention, (d) reproduction, and (e) motivation (Figure 1). However, while these factors are important aspects of learning, they are also influenced by behavior, social environment, and personal traits, such as cognition, beliefs, and skills (Schunk & Usher, 2019). The interdependencies between behavior, personality, and the environment concerning the learning process make the SCT an ideal theoretical framework for investigating how cyber-meddling impacts self-evaluation, values, and outcome expectations in voters.

***Figure 1**. Impact of Cyber-meddling on the voter decision-making process in national elections conceptual framework*



Nature of the Study

This study employs quantitative research methodology to examine the relationship between cyber election meddling by foreign governments and their impact on the voter decision-making process in government elections. Quantitative methods were deemed appropriate due to the need for statistical analysis of numerical data and hypothesis testing (Yilmaz, 2013). Quantitative research, emphasizing systematic measurement and statistical analysis, offers significant potential for generalizing findings across larger populations. By quantifying variables that describe the phenomenon under investigation, researchers can identify patterns, relationships, and trends beyond the specific sample studied (Savela, 2018; Yilmaz, 2013). This generalizability is achieved through rigorous sampling techniques and standardized data collection methods, ensuring that the results represent the target population (Abutabenjeh & Jaradat, 2018; Creswell, 2014). However, it is crucial to acknowledge the limitations of quantitative research, such as the potential for bias and the exclusion of contextual factors, which may impact the applicability of findings in certain situations. Nonetheless, the ability to generalize findings remains a crucial strength of quantitative research, enabling scholars to make inferences and predictions confidently.

The research design of this study is descriptive, non-experimental, and cross-sectional. Descriptive research provides a detailed description of variables and their characteristics, such as definitions, ranges, limitations, and units of measurement (Harkiolakis, 2017). The large amount of data generated by descriptive research helps make recommendations for practice (Moser & Korstjens, 2018; Savela, 2018; Taguchi, 2018). Delimitating the study subject to events related to and leading up to elections requires using a cross-sectional design, which captures a snapshot of the phenomenon and its interpretation at a specific time (Spector & Meier, 2014). Furthermore, this study focused on the population of voters in national elections, only including those who exercised their right to vote.

A non-probabilistic purposive sampling approach was employed, meaning that participants were selected based on specific criteria and qualifications to ensure a heterogeneous representation of the entire population. Participants were recruited through open invitations posted on Facebook, LinkedIn®, direct messaging, and email. Data was collected through an online questionnaire hosted on Google Forms, modeled after existing instruments previously used to measure perceptions and behaviors of participant attributes. The validity of the questionnaire was ensured through a review by a committee of experts and a pilot study. The data collected were analyzed using the Statistical Package for the Social Sciences (SPSS) version 28.

The statistical analysis included the one-sample chi-square test, the chi-square test for independence, and the Kruskal-Wallis test for variables that were not normally distributed. Spearman's rho was used to determine relationships and the strength of the relationships between the study variables. Furthermore, ethical and privacy issues were addressed as required by Ecole des Ponts Business School practices. Any surveys that were not fully completed were excluded from the analysis.

Research Questions

The following research question (RQ) guided the study:

RQ. Is there a relationship between voters' belief in cyber election meddling by foreign governments and their belief in its impact on their decision-making process in government elections?

Hypotheses

H_0: There is no relationship between voters' belief in cyber election meddling by foreign governments and their belief in its impact on their decision-making process in government elections.

H_a: There is a relationship between voters' belief in foreign governments' cyber election meddling and their belief in its impact on their decision-making process in government elections.

Significance of the Study

This study examines reported cyber-meddling and its effect on government elections like the 2016 U.S. Federal elections, the 2020 U.S. Federal elections, the 2016 Brexit referendum in the U.K., and the 2017 French presidential election. Against this background, this study determines whether cyber-meddling affected voters' decision-making process in election results. Furthermore, this study determined whether cyber-meddling impacted voters' perceptions of future elections. These findings may be crucial for shaping policies and interventions to restore trust in the electoral process.

Social media platforms play a significant role in shaping public opinion and facilitating communication. However, the rise of cyber-meddling has threatened the integrity and security of these platforms. The findings of this study can offer insights into how social media companies could implement robust measures for preventing election interference. Furthermore, the study's results could assist governments and policymakers in developing enforceable accounting strategies and mitigating the cyber-meddling threat in future elections on these platforms. Policymakers can use the results to create effective strategies for protecting future elections from cyber-meddling. At the same time, the public will be better informed about the risks posed by election interference on social media and the measures being taken to mitigate these risks. This study could represent an important step in restoring the public's trust in the electoral process and strengthening it for the years to come.

Definitions of Key Terms

Decision-making process: the cognitive and organizational procedures used by individuals and groups to evaluate alternatives, analyze risks, and determine the optimal course of action in various situations (Kahneman & Tversky, 1979).

Election Cyber-meddling refers to using computational technologies in cyberspace for malevolent and destructive purposes to transform, influence, or modify the election results for a particular country (Sander, 2019).

Government Elections: a recurring democratic process in which citizens vote to choose representatives and make decisions on public policies, guided by electoral systems and procedures (Powell & Powell Jr, 2000).

Voter perception: the subjective interpretation and understanding of political candidates, issues, and campaigns by individual voters, often influenced by various factors such as media, personal beliefs, and social interactions (Huddy et al., 2015).

Summary

Chapter 1 introduced some challenges that democracies continue to face with election meddling. The risk of election interference via new technologies and evolving tactics is a continuing challenge for democracies. As such, researchers, social media companies, and lawmakers must take steps to ensure that election meddling can be effectively addressed. It is essential to consider the attitudes and behaviors of voters exposed to such interference. Examining how election interference affects individuals' voting behavior may provide valuable information for creating more effective strategies and regulations to prevent future election meddling. For example, research may show that individuals subjected to deceptive ads or negative opinions on social media are more likely to change their voting behavior. By better understanding how voters process and use information from their social environment, researchers and lawmakers can develop more effective tools and policies to protect the integrity of democratic processes, including enacting laws that prevent or reduce the impact of future attempts at election interference.

This study examined the impact of election meddling on voters through the lens of the SCT. The SCT posits that individuals are heavily influenced by the information they receive from their social environment and that this information helps shape their attitudes, beliefs, and behaviors (Bandura & Walters, 1977). The population consisted of individuals who participated in a general election and were exposed to cyber-meddling. A descriptive, non-experimental, cross-sectional design was selected, and data collection relied on a self-administered survey instrument to gather participant data. A non-probabilistic purposive sampling method was employed to select participants from the identified population, ensuring that the participants were representative of the larger population of voters subjected to election meddling. Before collecting the data, a pilot study was conducted to verify the validity and reliability of the questionnaire used.

About The Author

Dr. Faton Aliu
Owner and President, PECB

With over 25 years of professional experience spanning quality and information security management, project management, IT, consulting, training, and auditing, Faton has consistently demonstrated a system-oriented approach and exceptional leadership. His tenure at PECB has been marked by significant achievements, where he has been instrumental in driving corporate goals and strategies and overseeing the entire workforce. Faton’s role involves providing inspirational leadership and direction to executives, fostering a culture of effective decision-making, and ensuring PECB's continued development toward achieving short- and long-term objectives.

Beyond his responsibilities at PECB, he serves on the Board of Directors of the International Personnel Certification Association (IPC) and contributes to Canadian committees/working groups for ISO/IEC 20000 and ISO/IEC 38500. His professional journey includes serving as the CEO of DCE Group, specializing in ISO standards implementation, and as the Educational Technologies Director at the American University in Kosova.

Faton holds a doctorate from École des Ponts Business School in Paris, a master’s degree in service management from the Rochester Institute of Technology, and executive certificates in Mergers and Acquisitions, Cybersecurity, and Open Innovation from Harvard University. Additionally, he holds certifications, including ISO/IEC 27001 Master, Quality Systems Manager, ISO 9001 Lead Auditor, ISO/IEC 20000 Implementer, ISO/IEC 27001 Lead Auditor, ISO/IEC 27001 Lead Implementer, and CE Marking Counselor. Faton is passionate about leveraging his expertise and experience to drive meaningful impact and growth in PECB and the broader professional community.

Contact the author:
faton.aliu@pecb.com
https://www.linkedin.com/in/fatonaliu/

About PECB

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Why Choose PECB?

At PECB, we are committed to your success. We work closely with you to understand your unique challenges and provide tailored training solutions that meet your specific needs. Our goal is to help you build a secure digital future, protect your business integrity, and ensure operational resilience.

Expertise and Accreditation:

At PECB, we blend deep expertise with globally recognized and accredited training portfolio. Our training courses are designed by industry leaders and adhere to the highest standards.

Flexible Learning Options:

We offer flexible learning options, allowing you to access our training programs online or in-person, so you can learn at your own pace.

Industry-Relevant Training:

Our training programs are continuously updated to reflect the latest industry trends and threats. This ensures that you receive the most current and relevant information to protect your organization effectively.

Global Reach:

Our extensive network of over 2,600 partners and 2,100 trainers globally, ensuring you receive top-tier training and support, no matter where you are located, providing you with consistent quality and accessibility.

PECB's Comprehensive Portfolio

We offer diverse education solutions designed to meet the demands of various industries and roles, ensuring Digital Trust.

The primary services are grouped as follows:

1. **Professional Courses:** Choose from over 300 tailored training courses to meet diverse industry needs and career levels. Whether you are just starting or seeking to advance your expertise, our diverse portfolio offers training courses designed to meet your goals.

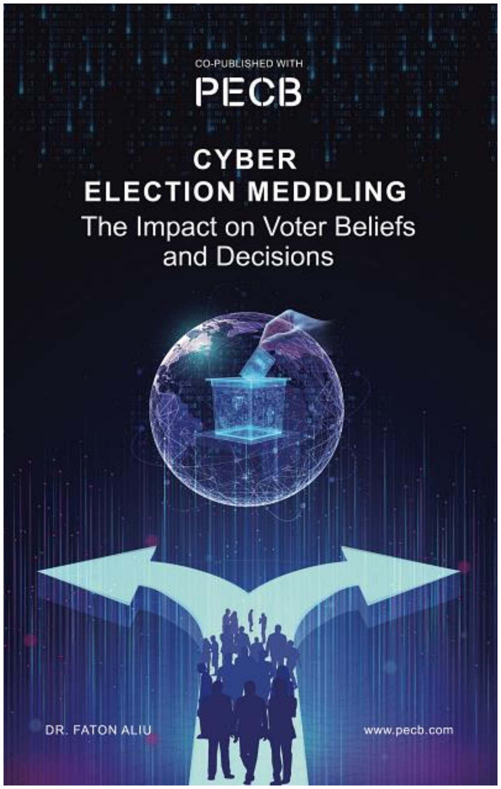
2. **Cybersecurity Technical Courses:** Delve into in-depth security courses with technical know-how and hands-on labs in a simulated environment that will prepare you for real-life challenges.

3. **PECB Skills:** Unlock a world of knowledge with expert-led video capsules and certificate programs, with select courses accredited by ANAB. These are perfect for continuous learning at your convenience!

4. **PECB Connect:** Take your auditing career to the next level by becoming a world-renowned Management System Auditor and joining the platform that serves as a bridge between certification bodies and auditors.

For more information, contact PECB at:
support@pecb.com
+1-844-426-7322
6683 Jean Talon E, Suite 336, Montreal, H1S 0A5, QC,
Canada, or reach out directly through our website
www.pecb.com.

We're here to support you every step of the way!



This research explores the effects of cyber election meddling on voter beliefs and decision making. It examines tactics, media influence, and implications for democratic integrity, providing insights into cybersecurity's role in elections.

Cyber Election Meddling:
The Impact on Voter Beliefs and Decisions
By Dr. Faton Aliu