International Journal of Educational Sciences and Arts (IJESA)
Vol. (4), No. (4)
IJESA
April 2025
المجلة الدولية للعلوم التربوية والآداب
الإصدار (4)، العدد (4)

Cybersecurity in Digital Diplomacy: A Comparative Analysis of the United States and Kingdom of Bahrain

Fawaz Bubshait
PhD in Digital Media and Communication Technology - International Diplomatic Relations, Bahrain
f.bubshait@gmail.com

Abstract

In an era of digital diplomacy, cybersecurity has become a critical component of international relations. As diplomatic engagements shift to digital platforms, the risks associated with cyber threats-ranging from espionage and misinformation to cyber warfare-have escalated. This study provides a comparative analysis of cybersecurity strategies in digital diplomacy between the United States and Kingdom of Bahrain, two nations with distinct geopolitical positions and technological capabilities. The research employs an empirical approach, integrating international case studies to assess how both countries address cybersecurity challenges in diplomatic interactions. The findings highlight key differences in policy frameworks, institutional capacities, and international collaborations, offering insights into the effectiveness of cyber diplomacy in securing national and global interests. The study also explores emerging trends and best practices, providing policy recommendations for strengthening cybersecurity in diplomatic affairs.

Keywords: Cybersecurity, Digital diplomacy, Cyber threats, U.S. Cyber strategy, Bahrain cyber policy, Cyber Norms, Cyber espionage.

Introduction

The increasing reliance on digital communication in international diplomacy has transformed the way states interact. While digital platforms provide efficiency and

accessibility, they also expose diplomatic channels to cyber threats, including espionage, data breaches, and misinformation campaigns. Cybersecurity is now an essential component of statecraft, shaping diplomatic engagements, strategic alliances, and national security policies.

This research examines the cybersecurity strategies of the United States, a global leader in cyber capabilities, and Kingdom of Bahrain, a key Middle Eastern player that has rapidly advanced its digital infrastructure. By comparing these two nations, this study aims to assess how different diplomatic approaches and cybersecurity policies impact national and international digital diplomacy efforts.

Research Objectives

This study aims to:

1. Compare the cybersecurity frameworks and digital diplomacy strategies of the **U.S. and Bahrain**.
2. Analyze international case studies to assess the effectiveness of different cybersecurity measures in diplomatic contexts.
3. Identify key challenges and opportunities in securing diplomatic communications.
4. Provide policy recommendations for enhancing cybersecurity in digital diplomacy.

Research Questions

- How do the U.S. and Bahrain approach cybersecurity in digital diplomacy?
- What role do international cyber threats and cyber norms play in shaping diplomatic strategies?
- What lessons can be drawn from international case studies to improve cybersecurity in diplomacy?

Methodology

This research follows an empirical approach, utilizing real-world data, government reports, and case studies from international cybersecurity incidents. The study employs a comparative framework to analyze legal policies, institutional strategies, and diplomatic initiatives undertaken by the U.S. and Bahrain. Case studies from global cybersecurity incidents are incorporated to contextualize findings and offer a broader perspective on cyber diplomacy.

Significance of the Study

Understanding how different nations integrate cybersecurity into diplomatic efforts is crucial for developing global cyber norms and cooperation mechanisms. This study provides valuable insights for policymakers, cybersecurity experts, and diplomats seeking to enhance cyber resilience in diplomatic engagements.

Cybersecurity Frameworks in Digital Diplomacy

Cybersecurity in digital diplomacy requires a robust legal and institutional framework to protect diplomatic communications and national interests. While the United States has long been a leader in cyber policy and cyber warfare capabilities, Kingdom of Bahrain has emerged as a regional digital hub, investing in cybersecurity to secure its diplomatic and economic interests. This chapter analyzes the legal frameworks, institutions, and strategic priorities of both nations.

The U.S. Cybersecurity Framework in Digital Diplomacy:

- National Cybersecurity Policies:

The United States has established a comprehensive cybersecurity strategy, integrating cyber defense into national security and diplomacy. Key components include:

International Journal of Educational Sciences and Arts, London Vol (4), No (4), 2025
https://doi.org/10.59992/IJESA.2025.v4n4p3 E-ISSN 2976-7237

- The National Cyber Strategy (2023): Focuses on securing critical infrastructure, countering cyber threats from state and non-state actors, and strengthening international partnerships.
- Cyber Diplomacy Act (2021): Established the Bureau of Cyberspace and Digital Policy to coordinate cyber diplomacy efforts.
- The CLOUD Act (2018): Facilitates international cooperation in cybercrime investigations.

- Cybersecurity Institutions:

The U.S. has multiple agencies overseeing cybersecurity and digital diplomacy:

- The Department of State's Bureau of Cyberspace and Digital Policy (CDP): Leads diplomatic efforts to establish global cyber norms.
- The Cybersecurity and Infrastructure Security Agency (CISA): Protects U.S. critical infrastructure and government networks.
- The National Security Agency (NSA): Conducts cyber intelligence and defense operations.

- International Cyber Diplomacy Initiatives:

The U.S. plays a key role in shaping global cyber governance, engaging in:

- The Paris Call for Trust and Security in Cyberspace
- The U.S.-EU Cyber Dialogue
- Cyber capacity-building programs in developing nations

- Case Study: U.S. Response to Russian Cyber Influence Operations:

The 2016 and 2020 U.S. elections witnessed large-scale cyber influence campaigns. In response, the U.S. implemented stricter cyber policies, sanctions, and diplomatic measures against cyber adversaries. This case highlights the U.S. approach to cybersecurity threats in diplomacy.

Bahrain's Cybersecurity Framework in Digital Diplomacy:

- National Cybersecurity Policies:

Bahrain has positioned itself as a digital leader in the Gulf region, prioritizing cybersecurity in its diplomatic and economic policies:

- National Cybersecurity Strategy (2017): Focuses on protecting national assets, promoting cyber awareness, and enhancing international cooperation.
- Personal Data Protection Law (PDPL, 2019): Aligns with global data protection standards (similar to the EU's GDPR).
- Cloud-First Policy (2017): Encourages secure digital transformation for government institutions.

- Cybersecurity Institutions:

Bahrain's cybersecurity governance is managed by:

- The National Cyber Security Center (NCSC): Oversees national cybersecurity policies and threat response.
- The Ministry of Foreign Affairs' Digital Diplomacy Unit: Manages cybersecurity in diplomatic affairs.
- The Telecommunications Regulatory Authority (TRA): Ensures cybersecurity compliance in Bahrain's digital infrastructure.

- International Cyber Diplomacy Initiatives:

Bahrain actively engages in:

- GCC Cybersecurity Cooperation: Regional collaboration on cyber threats.
- Partnerships with the U.S. on cyber defense and digital security.

- Bahrain's participation in global cybersecurity summits and initiatives.

- Case Study: Bahrain's Cyber Response to Regional Threats:

Bahrain has faced cyber threats from regional actors, including state-sponsored cyberattacks and disinformation campaigns. The government has strengthened cyber defenses, working closely with allies like the U.S. to mitigate risks.

Table (1): Comparative Analysis: U.S. vs. Bahrain in Cyber Diplomacy

Category	United States	Bahrain
Cybersecurity Policy Framework	Comprehensive, integrated into national security.	Focused on digital transformation and resilience
Institutional Structure	Multiple agencies (NSA, CISA, CDP) with specialized roles.	Centralized under NCSC and Ministry of Foreign Affairs
International Cyber Diplomacy	Active in shaping global cyber norms, alliances with NATO, EU.	Focused on regional cooperation (GCC) and partnerships with the U.S.
Cyber Threats & Response	Advanced cyber warfare capabilities, countermeasures against major cyber powers.	Faces regional cyber threats, collaborates with allies for security

Cybersecurity Challenges in Digital Diplomacy

As diplomacy moves into the digital sphere, cyber threats have evolved into a major concern for governments worldwide. Threat actors—including state-sponsored hackers, cybercriminals, and hacktivists—exploit vulnerabilities in diplomatic communication networks. The United States and Kingdom of Bahrain face distinct yet overlapping cybersecurity challenges in digital diplomacy. This section examines key threats, their impact on diplomatic relations, and the responses from both nations.

(1) Cyber Espionage and Data Breaches:

- Cyber Espionage Targeting U.S. Diplomacy:

The United States has been a primary target of cyber espionage by foreign actors. Some notable incidents include:

- Chinese cyber espionage campaigns targeting the U.S. Department of State and government officials (e.g., the OPM data breach in 2015).
- Russian cyber intrusions into diplomatic communications, as seen in the SolarWinds hack (2020), which compromised U.S. government agencies.
- Iranian cyber campaigns targeting U.S. diplomatic missions in the Middle East.

To counter such threats, the U.S. has implemented:

- Zero Trust Security Models for federal networks.
- Sanctions and diplomatic responses to cyber adversaries.
- Cyber threat intelligence sharing with allies.

- Cyber Espionage Risks for Bahrain:

As a strategic Gulf nation with strong alliances, Bahrain has faced cyber threats from regional actors. Key incidents include:

- Suspected Iranian cyber intrusions targeting Bahraini government and diplomatic entities.
- Advanced Persistent Threat (APT) groups attempting to breach Bahrain's digital infrastructure.
- Leaks of sensitive diplomatic communications through cyber espionage efforts.

Bahrain has strengthened its cyber defenses through:

- Cybersecurity partnerships with the U.S. and GCC nations.

- National cybersecurity drills and incident response frameworks.
- Enhancements in encryption and secure communication technologies.

(2) Disinformation and Cyber Influence Operations:

- U.S. Challenges with Disinformation in Digital Diplomacy:

The U.S. has been a primary target of foreign disinformation campaigns, particularly in:

- Election interference (e.g., Russian disinformation in 2016 and 2020).
- Social media manipulation targeting U.S. foreign policy narratives.
- Deepfake technology used to spread misinformation about diplomatic statements.

To address this, the U.S. has:

- Established the Global Engagement Center (GEC) to counter foreign disinformation.
- Pressured tech platforms (e.g., Facebook, Twitter) to combat fake news and foreign influence operations.
- Strengthened AI-driven misinformation detection systems.

- Disinformation Challenges in Bahrain:

Bahrain has faced regional disinformation campaigns aimed at:

- Destabilizing government credibility through fake news.
- Exploiting sectarian tensions using social media misinformation.
- Manipulating international narratives about Bahrain's human rights policies.

In response, Bahrain has:

- Developed digital literacy programs to counter misinformation.
- Partnered with regional cybersecurity agencies to track disinformation sources.
- Monitored online narratives to detect and mitigate influence operations.

Table (2): Comparative Summary of Cybersecurity Challenges

Cybersecurity Challenge	United States	Bahrain
Cyber Espionage	Faces threats from Russia, China, and Iran	Faces threats from regional actors (e.g., Iran)
Disinformation	Large-scale foreign influence operations, election interference	Regional disinformation campaigns targeting government credibility
Cyber Warfare	U.S. Cyber Command conducts offensive and defensive operations	Focused on defensive cyber measures, relies on GCC and U.S. support
Cyber Diplomacy Response	Establishes international cyber norms, sanctions adversaries	Strengthens regional cooperation and digital security partnerships

Case Studies in International Cyber Diplomacy

Examining international case studies provides valuable lessons on how nations handle cybersecurity challenges in diplomacy. This chapter analyzes three major incidents—each highlighting different aspects of cyber diplomacy, from cyberattacks on diplomatic institutions to coordinated cyber defense strategies. The cases offer insights applicable to the U.S. and Bahrain in strengthening cyber resilience.

Case Study 1: The 2018 Cyberattack on the U.S. State Department:

In 2018, the U.S. State Department suffered a massive cyber intrusion, suspected to be linked to a foreign state actor. The attack targeted the department's unclassified email systems, compromising sensitive diplomatic communications.

- Key Cybersecurity Failures:

- Weak Email Security Protocols: The attackers exploited vulnerabilities in unclassified government email systems.
- Lack of Real-Time Threat Detection: The breach was detected only after months of unauthorized access.
- Limited International Attribution Mechanisms: While intelligence agencies suspected Russian involvement; concrete attribution remained difficult.

- U.S. Cyber Diplomacy Response:

- Policy Reforms: The incident led to mandatory multi-factor authentication across all federal agencies.
- International Cyber Norms Advocacy: The U.S. pushed for stronger cyber accountability measures in United Nations cyber negotiations.
- Strengthened Cyber Alliances: The U.S. enhanced cyber intelligence-sharing agreements with allies.

- Relevance for Bahrain:

Bahrain can learn from this case by:

- Enhancing diplomatic email security to prevent espionage.
- Strengthening real-time cyber threat detection in government networks.
- Advocating for regional cyber norms within the Gulf Cooperation Council (GCC).

Case Study 2: The 2017 Qatar Diplomatic Crisis – Cyber Influence Warfare:

In 2017, a cyberattack on Qatar's state news agency (QNA) led to the publication of fabricated statements attributed to the Emir of Qatar. The false reports caused a

diplomatic crisis in the Gulf region, leading to a blockade by Saudi Arabia, the UAE, Bahrain, and Egypt.

- Cybersecurity and Diplomatic Failures:

- Misinformation Campaign: The attack manipulated digital media to influence regional diplomacy.
- Lack of Rapid Cyber Incident Response: Qatar was slow to contain the damage and verify the authenticity of the fabricated statements.
- Absence of Regional Cybersecurity Coordination: The crisis exposed the lack of a GCC-wide cyber diplomacy framework.

- Cyber Diplomacy Response:

- Qatar denied the statements and sought international mediation.
- The FBI and international cybersecurity firms investigated the cyberattack, later attributing it to a state-sponsored group.
- The incident prompted Qatar to heavily invest in cybersecurity infrastructure and AI-based misinformation detection.

- Lessons for the U.S. and Bahrain:

- For Bahrain: The incident underscores the importance of cyber resilience against influence warfare, especially in the Gulf region.
- For the U.S.: This case reinforces the need for stronger counter-disinformation strategies in digital diplomacy.

Case Study 3: The European Union's Cyber Diplomacy Toolbox:

In response to increasing cyber threats, the European Union (EU) introduced the Cyber Diplomacy Toolbox in 2017 to coordinate cyber responses across member states. The framework provides joint diplomatic, economic, and defensive measures against cyberattacks.

- Key Features of the Cyber Diplomacy Toolbox:

- Cyber Sanctions Mechanism: The EU can impose travel bans and asset freezes on cybercriminals.
- Cyber Threat Intelligence Sharing: Member states collaborate to counter cyber threats.
- Unified Diplomatic Response: The EU uses coordinated diplomatic channels to attribute and respond to cyber incidents.

- Notable Application: 2020 Sanctions on Russian Cyber Actors:

In 2020, the EU sanctioned six Russian individuals and organizations involved in cyber espionage and attacks on European institutions. The coordinated response demonstrated EU unity in cyber diplomacy.

- Relevance for the U.S. and Bahrain:

- For the U.S.: The Cyber Diplomacy Toolbox aligns with the U.S. push for global cyber norms and accountability.
- For Bahrain: The case highlights the benefits of regional cyber cooperation (e.g., a GCC cyber diplomacy framework).

Key Takeaways from International Case Studies:

- Cybersecurity Must Be Integrated into Diplomacy: Cyber threats are now central to diplomatic crises and must be addressed as part of foreign policy.
- International Cooperation Is Essential: Nations must engage in cyber intelligence sharing and collective diplomatic responses.
- Regional Frameworks Strengthen Cyber Resilience: The EU model can serve as inspiration for the U.S. in NATO and Bahrain in GCC cybersecurity cooperation.

- Misinformation and Cyber Influence Require New Diplomatic Strategies: The U.S. and Bahrain must prioritize counter-disinformation efforts as part of digital diplomacy.

Table (3): Comparative Summary of Case Studies

Case Study Key Cybersecurity Issue	Diplomatic Response	Lessons for the U.S. and Bahrain
U.S. State Department Attack (2018)	Cyber espionage targeting diplomatic emails	Cybersecurity reforms, international norms advocacy Strengthen email security, advocate for regional cyber norms
Qatar Diplomatic Crisis (2017)	Cyber influence warfare, misinformation international mediation, cybersecurity investments	Counter disinformation, improve cyber incident response
EU Cyber Diplomacy Toolbox (2017)	Coordinated cyber defense and response Cyber sanctions, intelligence-sharing	Develop regional cyber diplomacy frameworks (e.g., GCC cyber coordination)

Policy Recommendations for Strengthening Cybersecurity in Digital Diplomacy

Cyber threats are now a central challenge in diplomacy, affecting both major powers and smaller nations. This chapter presents policy recommendations for the U.S. and Bahrain, based on the cybersecurity challenges and case studies analyzed in previous chapters. The recommendations focus on strengthening national frameworks, enhancing cyber resilience in diplomatic communications, and improving international cooperation.

Recommendations for the United States:

1. Strengthening Cybersecurity in Diplomatic Communications:
   - Expand Zero Trust Security Policies across the Department of State's digital infrastructure.

- Enhance real-time threat detection with AI-driven cyber monitoring for diplomatic networks.
- Mandate end-to-end encryption for all diplomatic communications to prevent cyber espionage.

2. Improve Cyber Diplomacy Leadership:

- Expand the role of the Bureau of Cyberspace and Digital Policy (CDP) to lead global cyber norms discussions.
- Integrate cybersecurity into all U.S. diplomatic training programs to prepare diplomats for cyber threats.
- Advocate for a U.N. Cyber Accord to establish global cyber deterrence mechanisms.

3. Strengthening International Cyber Defense Cooperation:

- Deepen cyber intelligence-sharing agreements with Five Eyes, NATO, and the EU.
- Expand cybersecurity capacity-building programs for developing nations to strengthen global cyber resilience.
- Implement a coordinated cyber sanctions framework with allies to deter cyber adversaries.

4. Counter Disinformation in Digital Diplomacy:

- Develop an interagency task force to combat foreign disinformation campaigns targeting U.S. diplomatic efforts.
- Increase pressure on social media platforms to flag state-sponsored misinformation in real time.
- Strengthen AI-driven fact-checking systems to detect deepfake and manipulated content.

Recommendations for Kingdom of Bahrain:

1. Enhance National Cybersecurity Infrastructure:
   - Expand Bahrain's National Cyber Security Center (NCSC) to oversee all diplomatic cybersecurity operations.
   - Adopt Zero Trust Security principles for government networks to prevent cyber intrusions.
   - Mandate cybersecurity risk assessments for all digital diplomacy initiatives.
2. Strengthen Regional Cyber Diplomacy in the GCC:
   - Establish a GCC Cyber Diplomacy Framework to coordinate cybersecurity strategies across Gulf states.
   - Create a GCC-wide Cyber Incident Response Team (CIRT) to respond to cyber threats in diplomatic channels.
   - Develop joint GCC cyber exercises to test and improve collective cyber defense mechanisms.
3. Increase Collaboration with the United States:
   - Expand U.S.-Bahrain cybersecurity cooperation through bilateral agreements.
   - Host joint cyber diplomacy forums to align cybersecurity policies between the two nations.
   - Leverage U.S. expertise in counter-disinformation strategies to prevent cyber influence operations in Bahrain.
4. Invest in Cyber Education and Awareness:
   - Incorporate cybersecurity training into Bahrain's diplomatic education programs.

- Launch nationwide cyber awareness campaigns to prevent misinformation and cyberattacks.
- Encourage public-private partnerships to advance Bahrain's cybersecurity research and innovation.

Conclusion

This research has provided a comparative analysis of cybersecurity in digital diplomacy between the United States and Bahrain, integrating empirical data, international case studies, and policy recommendations. The findings reveal the following:

1. Cybersecurity is now a fundamental pillar of digital diplomacy:
   - Both state and non-state actors increasingly target diplomatic institutions through cyber espionage, data breaches, and disinformation campaigns.
   - As seen in the U.S. State Department cyberattack (2018) and the Qatar diplomatic crisis (2017), cybersecurity failures have direct diplomatic consequences.
2. The United States and Bahrain face distinct yet interconnected cybersecurity challenges:
   - The U.S. is targeted by global cyber adversaries (Russia, China, Iran) and faces foreign disinformation warfare in its diplomatic sphere.
   - Bahrain faces regional cyber threats, particularly from state-sponsored attacks and misinformation campaigns aiming to destabilize its diplomacy.
   - Both nations recognize cybersecurity as a diplomatic priority, leading to increased policy reforms and international collaborations.

3. International case studies highlight the importance of collective cyber defense:
   - The EU Cyber Diplomacy Toolbox demonstrates the effectiveness of coordinated cyber responses.
   - The Five Eyes intelligence-sharing model showcases the benefits of cyber intelligence cooperation among allies.
   - Bahrain could adopt regional cybersecurity frameworks similar to the EU model within the Gulf Cooperation Council (GCC).
4. Policy responses must evolve with emerging cyber threats:
   - The U.S. is enhancing its Zero Trust security frameworks, cyber deterrence strategies, and AI-driven disinformation detection.
   - Bahrain is investing in national cybersecurity capacity-building, regional cyber defense cooperation, and digital literacy initiatives.
   - Joint U.S.-Bahrain cyber diplomacy initiatives can further strengthen bilateral cybersecurity resilience.

Conclusion and Future Directions

- Cybersecurity in digital diplomacy is now a national security priority for both the U.S. and Bahrain.
- International cooperation is key—the U.S. and Bahrain must continue to expand their cybersecurity alliances.
- Emerging threats require adaptive policies—both nations should remain flexible in responding to evolving cyber challenges.
- Governments should integrate cybersecurity into national diplomatic strategies, ensuring that cyber resilience is a diplomatic priority.

- Cyber intelligence-sharing agreements, regional cyber cooperation, and diplomatic cyber norms must be strengthened.
- Cyber deterrence policies, including economic sanctions for cyber aggressors, should be internationally standardized.
- More empirical studies are needed to measure the effectiveness of cyber deterrence policies in diplomacy.
- Future research should explore AI-driven threat detection and predictive analytics for cybersecurity in diplomatic missions.
- The impact of quantum computing on diplomatic cybersecurity should be examined as technology advances.

References

- Atlantic Council. (2023, May 23). Cybersecurity creates new horizons for Abraham Accords. Atlantic Council. Retrieved from https://www.atlanticcouncil.org/event/cybersecurity-creates-new-horizons-for-abraham-accords/
- Biden, J. (2025). Executive Order on Improving the Nation's Cybersecurity. The White House. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2025/01/15/executive-order-on-improving-the-nations-cybersecurity/
- Blinken, A. J. (2024). United States International Cyberspace & Digital Policy Strategy. U.S. Department of State. Retrieved from https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/
- Coker Jr., H. (2024). White House Takes Aim at Internet Security. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/white-house-takes-aim-at-internet-security-78103a69
- IE University. (2024). Cyber diplomacy and cybersecurity: Guardians of the digital realm. IE Insights. Retrieved from https://www.ie.edu/uncover-ie/cyber-diplomacy-and-cybersecurity-guardians-of-the-digital-realm/

- Kaska, K., & Vihul, L. (2023). Cyber Diplomacy in the USA. Cyber Diplomacy Toolbox. Retrieved from https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy_USA.html
- Neuberger, A. (2025). Biden's new executive order aims to shore up US cyber defenses. AP News. Retrieved from https://apnews.com/article/3fc53784ad9d1c05d7de85224a762a36
- Politico. (2024, September 5). US, allied nations accuse Russia of cyberattacks against Ukraine and NATO. Politico. Retrieved from https://www.politico.com/news/2024/09/05/us-allied-nations-russia-cyberattacks-ukraine-nato-00177542
- ResearchGate. (2024). Bridging the Gap: An Analysis of Cybersecurity in Web Technologies for Cyber Diplomacy. ResearchGate. Retrieved from

  https://www.researchgate.net/publication/385297449_Bridging_the_Gap_An_Analysis_of_Cybersecurity_in_Web_Technologies_for_Cyber_Diplomacy
- U.S. Department of State. (2025). U.S. Security Cooperation with Bahrain. U.S. Department of State. Retrieved from https://www.state.gov/u-s-security-cooperation-with-bahrain/
- Wired. (2024). Antony Blinken Dragged US Diplomacy Into the 21st Century. Even He's Surprised by the Results. Wired. Retrieved from https://www.wired.com/story/big-interview-antony-blinken