FBI Open Up: Federal Bureau of Investigation

Thomas Jefferson Model United Nations Conference

TechMUN XXXI

High School Specialized Agency

Co-Chairs: Neha Chandran & Tejavi Kumar

Thomas Jefferson High School for Science and Technology

Dear Delegates,

Welcome to the FBI Open Up: Federal Bureau of Investigation in TechMUN XXVI! We are beyond excited to hear your debate on these two recent issues that are crucial to the future of our nation's safety. This committee takes place today, and focuses on issues relevant to our future. Each delegation in this committee represents a different individual playing an important role in the operation of the FBI, and each is expected to reflect on their views and the vision of the FBI. Be sure to bring those views and ideologies into TechMUN XXVI weekend. The first topic focuses on the usage of quantum algorithms as a safety defense, and the second topic looks into how we can address conspiracy theories behind Area 51.

As your chairs, we are looking for delegates with good background knowledge, calls to action in speeches, and integration of ideas into working papers within blocs. Each delegation has a specialty- we want to see collaboration while keeping your delegation's role in the FBI in mind. Even if you don't give many moderated caucuses, we want you to be active during unmoderated caucuses and voice unique ideas then. Remember- relevancy in committee is key!

With that being said, both of us hope that we can make your experience in committee as close to real life as possible with some fun involved. Through this experience, we want you to grow as delegates and explore your role in the FBI while taking risks by raising your placard and using intelligent hooks. We want you to leave this conference as delegates who can be confident in their ideas and communicate them to the world. If you have any questions at all, please do not hesitate to email us at fbiopenuptechmun2024@gmail.com, and we look forward to seeing you at TechMUN XXVI!

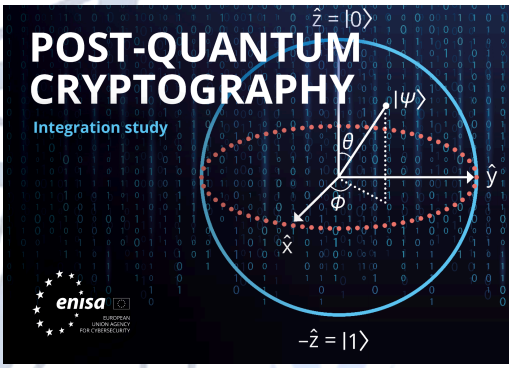
Neha Chandran and Tejavi Kumar

Co-Chairs, FBI Open Up: Federal Bureau of Investigation

Topic 1: Enforcing Security Measures by Investigating the Usage of Quantum Algorithms

Background

Quantum computing is an emerging field of technology with processing power far beyond what is offered by classical computing. By leveraging the principles of quantum mechanics, quantum computers operate in a fundamentally different way than classical computers, utilizing quantum bits of information (called "qubits") to simultaneously encode large amounts of data. One of the most discussed impacts of quantum computing is its potential to crack RSA encryption, a common method used to secure data. Decrypting would require the ability to factor a large number, an extraordinarily challenging task that would traditionally take millions of years for a classical computer to solve. Quantum computing, however, introduces algorithms such as Shor's algorithm, that can factor these numbers in a matter of a few hours. This capability threatens to make RSA and similar encryption methods vulnerable, enabling hackers to expose private data without authorization.



While such algorithms are still in their development stage and not yet deployed practically, there has still been significant concern among cybersecurity experts regarding the threat of quantum computing. In theory, quantum computers could break much of the encryption currently safeguarding the internet, financial transactions, and classified communication. To prevent this, countries all over the globe – most prominently the US and China – are racing to develop quantum-resistant cryptography, aiming to secure data while maintaining compatibility with existing frameworks.

As quantum computing research has been rapidly progressing, the timeline for when these machines will be capable of infiltration remains subject to debate. This event, dubbed as “Q-Day”, could arrive as soon as 2025 or may come closer near the middle of the century. The threat, however, has been taken into serious consideration, as stakeholders have been working together to prepare a post-quantum cryptographic landscape. This includes the development of new encryption standards that can resist quantum attacks and the implementation of “unhackable” protocols like quantum key distribution (QKD) that enable fully secure transactions.

Relevant Issues

One specific issue pertains to the vast amount of data the FBI collects, stores, and shares across different governmental and law enforcement organizations (authorized stakeholders, of course). This data often includes sensitive personal information, intelligence on criminal activities, and sometimes even communications relating to national security. To ensure its protection, the data is encrypted using the methods outlined above, which traditionally served as a viable option. Quantum computing's ability to break such encryption could expose this information, leading to privacy breaches.

Another challenge is the “harvest now, decrypt later” mindset among attackers. This strategy makes it possible for attackers to store currently unreadable encrypted data and wait until an algorithm strong enough has been created to decrypt. This is particularly appealing in the context of quantum cryptography, as hackers can “harvest” the necessary information beforehand and wait until the right technology is readily available to decrypt the data. Of course, this

technique is not standalone, as some encrypted information now may not be relevant (or even private for that matter) in the future.

Past and Current Action

In response to these challenges, the FBI, alongside other national security agencies, is investing in research and development of quantum-resistant encryption technologies. This includes participation in initiatives led by the National Institute of Standards and Technology (NIST) to standardize post-quantum cryptographic algorithms. In 2018, the National Quantum Initiative Act (NQI) was passed by both the House of Representatives and the Senate, giving permission to the United States to continue research in quantum computing technologies, with an emphasis on ensuring security measures. That same year, NIST launched Quantum Economic Development Consortium (QED-C) as an effort to enhance the quantum computing industry. Later, in 2022, the White House Memo NSM-8 outlined the goals for moving toward post-quantum cryptography.

Possible Solutions

From a scientific standpoint, the FBI can invest in quantum key distribution (QKD) technologies, which theoretically offer an unbreakable method of secure communication. The protocol involves the secure transfer of cryptographic keys between two parties (famously, Alice and Bob). One example, the BB84 protocol, involves using the principle of measurement to detect interference of a quantum state. A lesser known example, the E91 protocol, relies on the instantaneous correlations due to the principle of quantum entanglement to detect inference. By implementing QKD for its most sensitive communications, the FBI can ensure what is currently believed to be the highest level of security. However, we urge you to consider the practicality of

this solution: the hardware of quantum computing is still not advanced enough to carry out such operations on a large scale. Additionally, you will have to consider what stakeholders will be involved to actually implement this in the FBI.

Beyond adopting new technologies, the FBI can enforce stricter "cyber hygiene" to avoid internal privacy breaches and espionage. This includes regular audits of its cryptographic practices, the rewriting of particularly vulnerable algorithms, and the implementation of multi-factor authentication and other security measures that don't solely rely on encryption. These practices can help mitigate the threat of quantum computing (and other risks as well) in the FBI.

Questions to Consider

1) What new technologies or algorithms can be developed to counter the growing threat of quantum cryptography? How can the FBI actually implement these in practice?
2) What standards, guidelines, or plans should the FBI make to help ensure a post-quantum cryptographic landscape? How should they enforce these deliverables?
3) Is the current legislation provided by NSM-10 feasible for the long term? If not, how can we update these standards to fit future needs?
4) Who are the stakeholders involved in this process? Is additional government intervention required?

Helpful Links

https://www.qusecure.com/us-government-quantum-timeline/

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/

Works Cited

House, The White. “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems.” *The White House*, 4 May 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

“National Quantum Initiative Advisory Committee.” *National Quantum Initiative*, https://www.quantum.gov/about/nqiac/. Accessed 20 Mar. 2024.

“Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now.” *National Security Agency/Central Security Service*, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3498776%2Fpost-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now%2F. Accessed 20 Mar. 2024.

Topic 2: Addressing Conspiracy Theories Behind Area 51

Background

Located in the remote expanse of the Nevada desert, Area 51 has become synonymous with secrecy, leading to a broad spectrum of speculative narratives ranging from extraterrestrial encounters to advanced military experiments. Established during the height of the Cold War in the early 1950s, this U.S. Air Force facility, officially known as the Nevada Test and Training Range, initially served as a covert testing ground for cutting-edge aircraft and experimental technology. Since then, the history of Area 51 has been associated with the evolution of aerospace engineering, playing a pivotal role in the development and testing of groundbreaking aircrafts, including the iconic U-2 spy plane. Its remote location, shielded from public scrutiny, facilitated the pursuit of classified projects that pushed the boundaries of military and technological capabilities. As the Cold War ended and the world transitioned into a new era, Area 51's significance expanded beyond its military origins. The facility became a focal point for speculation and intrigue, with a pop culture narrative emerging around UFOs, extraterrestrial encounters, and alleged government cover-ups. The blending of classified technology and speculative misinformation has transformed Area 51 into a symbol that extends beyond the realm of military installations.

The FBI, our national law enforcement agency, stands at the forefront of ensuring national security and upholding the rule of law. The FBI's mandate encompasses a wide array of responsibilities, including counterterrorism, counterintelligence, criminal investigations, and cybersecurity. With a commitment to transparency, the FBI plays a crucial role in addressing public concerns, mitigating misinformation, and safeguarding the nation's interests.

Relevant Issues

There are a multitude of issues that contribute to the secrecy, public perception, and the broader implications of classified government activities surrounding Area 51. The persistent secrecy of Area 51 stands out as a central concern. The facility's lack of transparency regarding its activities has created an environment where speculation and conspiracy theories thrive. This opacity creates mistrust between the government and the public. Given the classified nature of certain activities at Area 51, concerns arise about public emergency preparedness. In the event of unforeseen incidents, the public's ability to respond appropriately and authorities' ability to communicate effectively become critical issues. Linked closely to this is the prevalence of public speculation and conspiracy theories surrounding Area 51. Ranging from alleged extraterrestrial encounters to advanced military experiments, these theories not only contribute to public confusion but can also have implications for national security. The media plays a big role in this and adds chaos to the confusion, so addressing this issue is also of concern. Furthermore, the impact of Area 51 on local communities, both environmentally and socially, is an important issue. Concerns exist about the potential environmental consequences of military testing, as well as the impact on the health and well-being of those living in proximity to the facility. Striking a balance between the need for security and the well-being of local communities is a crucial consideration.

Possible Solutions

Recognizing the intricate nature of the topic, the committee must craft solutions that address both the immediate concerns of the public and the long-term imperative of maintaining national security. A multifaceted approach is necessary, incorporating elements of transparency, strategic communication, and collaboration with experts. Transparency initiatives could involve selectively declassifying information, ensuring that the release of details does not compromise ongoing security protocols. Collaboration with scientific communities and reputable institutions is instrumental in establishing a foundation of credibility. Expert insights into the technological advancements and experiments conducted at Area 51 can serve to demystify the facility while fostering an environment of trust.

Questions to Consider

1) How can the FBI address conspiracy theories without compromising national security and classified information?
2) What steps can be taken to enhance transparency regarding the activities at Area 51 while ensuring the safety of ongoing operations?
3) In what ways can the committee leverage social media and online platforms to counteract misinformation and engage with the public?
4) Should the FBI consider declassifying certain information to address specific public concerns without compromising overall security?
5) How can the committee foster collaboration with scientific communities and experts to provide credible, verifiable information regarding Area 51?

Helpful Links

https://www.fbi.gov/

https://time.com/5627694/area-51-history/

https://vault.fbi.gov/storm-area-51

https://www.militarytimes.com/off-duty/military-culture/2023/01/26/how-area-51-became-a-hotbed-for-conspiracy-theories/

Works Cited

Area 51 Conspiracy Theories: Aliens in the United States | Britannica. https://www.britannica.com/video/212132/Area-51-military-air-force-base-alien-video. Accessed 20 Mar. 2024.

"Conspiracy Theories - TIME." *Time*, 20 Nov. 2008. *content.time.com*, https://content.time.com/time/specials/packages/article/0,28804,1860871_1860876_1861006,00.html.

F, et al. "Area 51 'Uncensored': Was It UFOs Or The USSR?" *NPR*, 17 May 2011. *NPR*, https://www.npr.org/2011/05/17/136356848/area-51-uncensored-was-it-ufos-or-the-ussr .

Is the Government Lying About Area 51? | The Psychology of Extraordinary Beliefs. https://u.osu.edu/vanzandt/2019/04/12/is-the-government-lying-about-area-51/. Accessed 20 Mar. 2024.

published, Robert Lea. "Area 51: What Is It and What Goes on There?" *Space.Com*, 11 Apr. 2022, https://www.space.com/area-51-what-is-it.

Sicard, Sarah. "How Area 51 Became a Hotbed for Conspiracy Theories." *Military Times*, 26 Jan. 2023, https://www.militarytimes.com/off-duty/military-culture/2023/01/26/how-area-51-became-a-hotbed-for-conspiracy-theories/.

Dossier

1. Director of the Federal Bureau of Investigation (FBI) - Christopher Wray
2. Deputy Director of the FBI - Paul Abbate
3. Associate Deputy Director - Brian C. Turner
4. Chief of Staff - Jonathan Lenzner
5. Former FBI Executive: Independent Consultant - Christopher Gay
6. Attorney General - Merrick Garland
7. Deputy Attorney General - Lisa Monaco
8. Associate Attorney General - Benjamin C. Mizer
9. Secretary of Homeland Security - Alejandro Mayorkas
10. Information Management Division - Shannon Parry
11. Insider Threat Office – Janeen DiGuiseppi
12. Inspection Division – William J. DelBagno (Acting)
13. Finance and Facilities Division - Nicholas Dimos
14. Office of the Chief Information Officer – Jeff Bauerlein
15. President of the United States - Joe Biden
16. Vice President of the United States - Kamala Harris
17. Office of Congressional Affairs – Patrick Findlay
18. Office of Diversity and Inclusion – Katherine Wood (Acting)
19. Office of EEO Affairs – Karen Corado (Acting)
20. Office of the General Counsel – Jason A. Jones
21. Office of Integrity and Compliance – Catherine Bruno
22. Office of Internal Auditing – Cindy Hall (Acting)
23. Office of the Ombudsman – Chauncenette Morey (Acting)
24. Office of Professional Responsibility – Ben L. Beyers II (Acting)
25. Office of Public Affairs – Cathy L. Milhoan
26. Secretary of Defense – Lloyd J. Austin III
27. Deputy Secretary of Defense – Kathleen H. Hicks
28. Chairman of the Joint Chiefs of Staff Air Force General – Charles Q. Brown, Jr.
29. Vice Chairman of Joint Chiefs of Staff Navy Admiral – Christopher W. Grady
30. Chief of National Security Agency – General Timothy D. Haugh
31. Deputy Director of National Security Agency – Wendy Noble
32. Executive Director of National Security Agency – Catherine Aucella
33. Chief of Staff of National Security Agency – Marlisa L. Smith
34. Deputy Chief of Central Security Service – Matteo Martemucci
35. Senior Enlisted Advisor of National Security Agency/Central Security Service – Kenneth M. Bruce, Jr.
36. Secretary General of INTERPOL – Jürgen Stock
37. President of INTERPOL – Ahmed Naser Al-Raisi

38. Vice President of INTERPOL – Sarka Havrankova
39. Vice President of INTERPOL – Garba Baba Umar
40. Vice President of INTERPOL – Valdecy Urquisa