Threat Landscape for GCC Students in the UK

By Catherine Perez-Shakdam and Aurele Tobelem

Table of Contents:

Executive Summary

Gulf Cooperation Council (GCC) students—originating from Bahrain, Kuwait, Oman, Saudi Arabia, and the United Arab Emirates—face an escalating cybersecurity threat while studying in the United Kingdom. As members of politically connected families and future national leaders, they are prime targets for hostile state actors, particularly Iran, which seeks to infiltrate their digital infrastructure for espionage, influence, and coercion.

Iranian cyber units, including those operating under the Islamic Revolutionary Guard Corps (IRGC) and Ministry of Intelligence and Security (MOIS), deploy highly sophisticated tactics such as phishing attacks, spyware, social engineering, and blackmail to compromise students' communications. These threats extend beyond financial cybercrime; they are part of Iran's broader geopolitical strategy to undermine GCC states, monitor diaspora communities, and cultivate assets for long-term intelligence objectives.

Key Cyber Threats

1. **Phishing & Credential Theft** – State-backed hackers craft deceptive emails impersonating universities and trusted organizations to steal student credentials and gain access to private communications.
2. **Malware & Spyware Deployment** – Students' devices are infected via malicious links or apps, allowing attackers to monitor calls, track locations, and extract sensitive data.
3. **Social Engineering & Digital Manipulation** – Iranian operatives pose as academics, recruiters, or journalists to establish trust before extracting personal or politically relevant information.
4. **Surveillance & Blackmail** – Compromised data is used to monitor, pressure, or coerce students into compliance with hostile intelligence objectives.

Strategic & Geopolitical Implications

Iran's cyber-espionage campaign against GCC students is not random; it serves critical intelligence functions, including:

- **Espionage & Data Collection:** Monitoring students from influential families to gain insights into Gulf state affairs.
- **Ideological Influence:** Recruiting sympathizers who may later assume leadership positions within GCC governments or security agencies.
- **Long-Term Strategic Leverage:** Exploiting compromised individuals for future intelligence operations.

The cyber threat landscape is further complicated by diplomatic tensions between Iran and the Gulf states, making Iranian cyber operations a direct challenge to UK-GCC security cooperation.

Mitigation Strategies

A multi-layered defence approach is necessary, involving students, universities, and governmental institutions:

For Students:

- Implement strong passwords and two-factor authentication (2FA).
- Avoid clicking on unknown links or downloading suspicious files.
- Use encrypted communication channels and avoid public Wi-Fi.
- Limit social media exposure to reduce risk of targeting.
- Report any suspicious cyber activity to university IT departments.

For Universities:

- Conduct cybersecurity training tailored for high-risk international students.
- Strengthen network security and monitor for anomalies in data traffic.
- Establish clear reporting channels for students facing cyber threats.
- Limit public exposure of student data to prevent reconnaissance by hostile actors.

For UK & GCC Governments:

- Expand intelligence-sharing on Iranian cyber tactics targeting GCC nationals.
- Strengthen counter-espionage laws to criminalize cyber-enabled recruitment.
- Enhance diplomatic pressure on Iran to deter state-sponsored cyber intrusions.
- Provide pre-departure cybersecurity briefings for GCC students studying abroad.

The persistent cyber-espionage targeting GCC students in the UK is not merely a privacy concern but a national security issue with long-term strategic consequences. If left unchecked, these operations could lead to political blackmail, recruitment of informants, and erosion of trust within Gulf leadership circles.

A coordinated defence—combining individual cybersecurity vigilance, institutional safeguards, and national security interventions—is essential to counter these threats. By implementing these measures, the UK and its GCC allies can ensure that students remain protected from foreign surveillance, manipulation, and coercion—preserving both academic integrity and geopolitical stability.

Introduction

Foreign students from the Gulf Cooperation Council (GCC) nations—Bahrain, Kuwait, Oman, Saudi Arabia, and the United Arab Emirates (excluding Qatar)—face an increasingly sophisticated and persistent cybersecurity threat while pursuing their studies in the United Kingdom. Many of these students come from politically influential families or are positioned to assume leadership roles within their respective countries, making them prime targets for state-backed cyber-espionage. Among the most active and persistent adversaries, the Islamic Republic of Iran has demonstrated a strategic commitment to monitoring, infiltrating, and coercing individuals connected to Middle Eastern affairs, deploying its cyber units to compromise students' digital and personal security.

Iranian cyber operations, conducted through both formal intelligence agencies and paramilitary cyber units such as APT42[1], target GCC students as part of Tehran's broader regional strategy. These operations extend beyond conventional cybercrime, representing a concerted effort to gather intelligence, exert ideological influence, and recruit or coerce individuals who may later occupy influential positions in Gulf governments, security institutions, or corporate sectors. The cyber tactics employed—ranging from phishing and malware deployment to social engineering and coercion—are not opportunistic but highly tailored, often spanning months of surveillance, relationship-building, and digital exploitation.

This report provides a comprehensive analysis of the principal cyber threats facing GCC students in the UK, detailing the methodologies employed by hostile cyber actors, the vulnerabilities within academic institutions and digital platforms, and the broader geopolitical imperatives driving these espionage efforts. It also outlines key mitigation strategies aimed at strengthening the cybersecurity resilience of this vulnerable cohort.

Unlike financially motivated cybercriminals, state-backed intelligence services such as those operating under Iran's Revolutionary Guard Corps (IRGC) and Ministry of Intelligence and Security (MOIS) engage in persistent, highly tailored techniques designed to compromise specific individuals over extended periods. These attacks, which exploit digital, social, and psychological vulnerabilities, are primarily executed through five key vectors:

1. **Targeted Phishing and Credential Theft[2]:**
   Highly convincing phishing campaigns impersonate academic institutions, government bodies, and professional organizations to harvest credentials. These attempts often align with students' affiliations and interests, increasing their effectiveness. Once credentials are compromised, adversaries gain unrestricted access to private communications, personal documents, and social media

[1] Google Cloud. "Untangling Iran's APT42 Operations." *Google Cloud Blog*, February 28, 2024. https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations.
[2] Palo Alto Networks. "What Is a Credential-Based Attack?" *Palo Alto Networks*, accessed March 5, 2024. https://www.paloaltonetworks.co.uk/cyberpedia/what-is-a-credential-based-attack.

accounts—granting them the ability to monitor, manipulate, and exploit their targets.

2. **Malware Deployment and Spyware Intrusions[3]:**
   State-sponsored cyber units deploy sophisticated malware and spyware through malicious links, compromised applications, and trojanized software disguised as VPN services or encrypted messaging platforms. Once installed, these tools provide adversaries with deep access to a student's device, allowing them to intercept messages, record calls, activate microphones and cameras, and track real-time location data. Iranian-backed cyber groups have developed spyware capable of GPS tracking, keystroke logging, and data exfiltration, transforming compromised devices into tools of surveillance and coercion.
3. **Social Engineering and Digital Manipulation:**
   Beyond technical exploits, Iranian cyber operatives leverage social engineering techniques to extract information and gain access to student networks. Posing as fellow students, journalists, recruiters, or think-tank representatives, these operatives initiate prolonged interactions designed to establish trust and credibility. Over time, these engagements escalate into requests for seemingly innocuous favors—such as downloading a "security update" or sharing non-classified documents—that serve as the gateway for deeper intelligence-gathering efforts.
4. **Surveillance and Intelligence Collection:**
   A successfully compromised device provides adversaries with real-time intelligence on a student's movements, affiliations, and political inclinations. Advanced surveillance malware enables hostile actors to monitor encrypted conversations, extract sensitive files, and analyze behavioral patterns to identify potential pressure points. This intelligence is then used to map out personal and professional networks, assess vulnerabilities, and, in some cases, preemptively suppress anti-Iranian narratives or Gulf-backed initiatives.
5. **Coercion and Digital Blackmail:**
   The accumulation of personal data allows adversaries to engage in coercion, leveraging compromising material—ranging from personal relationships to politically sensitive statements—to exert pressure on targeted individuals. The threat of exposure, whether to family members, employers, or government authorities, can force compliance, ideological conformity, or even recruitment into intelligence operations. Even in the absence of direct coercion, the mere perception of surveillance fosters self-censorship, effectively neutralizing individuals from engaging in political discourse or policy activism.

The cybersecurity risks facing GCC students in the UK must be understood within the broader framework of Iranian strategic objectives. Unlike conventional cybercriminals, Iranian-backed cyber units operate with the express purpose of:

---

[3] National Cyber Security Centre (NCSC). "Mitigating Malware and Ransomware Attacks." *National Cyber Security Centre (UK)*, accessed March 5, 2024. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks.

- Monitoring political dissidents and diaspora communities perceived as ideological or security threats to Tehran.
- Gathering intelligence on Gulf state personnel and future leaders likely to influence national policies in security, energy, and foreign relations.
- Undermining Gulf state influence in the media, diplomatic, and policy spheres by suppressing narratives that challenge Iranian geopolitical interests.

British intelligence agencies have consistently warned of the evolving cyber threat posed by Iranian actors[4], noting their ability to engage in both technical cyber operations[5] and hybrid influence campaigns. The persistent targeting of GCC nationals aligns with Tehran's broader geopolitical objectives, particularly as the Gulf region continues to play a pivotal role in regional security, global energy markets, and counterterrorism initiatives. Given the strategic significance of these students—both as current intelligence assets and as future policymakers—Tehran's interest in their digital and personal vulnerabilities is unlikely to wane.

This report underscores the need for heightened awareness and proactive security measures among GCC students, academic institutions, and governmental bodies. While the digital threat landscape is evolving, a combination of cybersecurity best practices, institutional safeguards, and international cooperation can mitigate these risks—ensuring that students can pursue their academic ambitions free from the specter of foreign surveillance, manipulation, or coercion.

Tactics Used by Hostile State Actors

Hostile state actors, particularly Iran, employ a sophisticated blend of technical cyber exploits[6] and psychological manipulation to compromise the devices and digital accounts of GCC students studying in the United Kingdom. These operations are designed to enable surveillance, coercion, and influence, with long-term strategic objectives. The primary tactics include:

Spear Phishing and Credential Harvesting

---

[4] *Daily Express.* "Iran Spy Who 'Poses Threat to UK' Could Be Released from Jail in Days." *Express.co.uk*, February 29, 2024. https://www.express.co.uk/news/politics/2022612/iran-spy-jail-threat-uk.

[5] National Cyber Security Centre (NCSC). "UK and US Issue Alert as Cyber Actors Working on Behalf of the Iranian State Carry Out Targeted Phishing Attacks." *National Cyber Security Centre (UK)*, February 21, 2024. https://www.ncsc.gov.uk/news/uk-us-issue-alert-cyber-actors-behalf-iranian-state-carry-targeted-phishing-attacks.

[6] Computer Weekly. "UK on High Alert over Iranian Spear Phishing Attacks, Says NCSC." *Computer Weekly*, February 21, 2024. https://www.computerweekly.com/news/366612026/UK-on-high-alert-over-Iranian-spear-phishing-attacks-says-

State-backed cyber units deploy highly targeted phishing campaigns, known as spear phishing, to deceive students into divulging login credentials. Unlike mass phishing attempts, these operations are meticulously crafted to appear credible, often impersonating university officials, colleagues, or even family members. Iranian cyber units have previously sent students emails purporting to be from academic administrators or trusted professors, requesting login verification for university portals or document access. The email directs recipients to a fraudulent but convincingly designed webpage that captures usernames, passwords, and multi-factor authentication codes.

Iranian threat actors have been known to impersonate journalists, academic researchers, or conference organisers to engage in extended discussions with students before deploying malicious links. A documented case in 2022 attributed to Iran's APT42 cyber unit involved WhatsApp messages inviting scholars focused on Middle Eastern affairs to a fabricated academic conference. The registration link redirected victims to a fake Google login page that harvested their credentials. Once access is obtained, attackers can read private emails, reset passwords, and monitor future correspondence, facilitating continued espionage and potential manipulation.

Malware Infection via Links and Applications

Malware deployment remains a cornerstone of Iranian cyber operations. Attackers frequently disguise spyware as legitimate documents, software updates, or VPN services to entice targets into installation. A common technique involves sending links to supposed research papers or security tools, which, when opened, execute hidden spyware installations.

Iranian cyber units have been identified using SMS-based malware distribution, where victims receive messages containing links to purportedly popular VPN applications. In reality, clicking these links installs spyware that grants full access to the student's device. Once infected, attackers can log keystrokes, capture screenshots, steal files, and even activate cameras and microphones. Investigations by cybersecurity firms such as Mandiant have revealed that Iranian spyware can track GPS location in real time and intercept private communications without detection.

The covert nature of these intrusions makes them particularly effective. Advanced malware can remain undetected for extended periods, allowing continuous intelligence collection. Iranian cyber units have employed these techniques since at least 2015, targeting political dissidents and regional figures, and the same methods can easily be applied to GCC students abroad.

Social Engineering and Digital Manipulation

Beyond direct technical intrusions, adversarial actors rely heavily on social engineering tactics to manipulate targets into unwittingly compromising their security. Iranian operatives have been known to create fake identities on professional and social networking platforms such as LinkedIn, Telegram, and Facebook. A GCC student might

be approached by an individual posing as a fellow expatriate, a recruiter offering an attractive employment opportunity, or a journalist seeking insights into Gulf affairs.

These interactions can span weeks or even months, gradually building trust before the target is encouraged to open a malicious link or download an infected document. In a documented case, Iranian hackers masqueraded as British academics from the School of Oriental and African Studies (SOAS), inviting Middle East scholars to an online event. The operation was reinforced by a fabricated webpage on a university-affiliated media site, lending credibility to the deception. After multiple exchanges, the victims were directed to a registration portal that harvested their credentials.

Social media surveillance further amplifies these risks. GCC students who publicly express political views or share personal information may inadvertently provide attackers with intelligence to refine phishing lures or identify pressure points for coercion. Any digital platform where students engage in discussions or networking presents a potential avenue for manipulation.

Surveillance Software and Mobile Monitoring

State-backed cyber units rely on sophisticated spyware tools to maintain persistent surveillance over compromised targets. Once installed, these programs enable continuous real-time monitoring of a student's communications, movements, and online activities. Iranian groups affiliated with the Islamic Revolutionary Guard Corps (IRGC), such as APT42, have developed mobile spyware capable of intercepting calls and messages, remotely activating device microphones, and tracking location history.

The extensive digital footprint stored on mobile devices makes students particularly vulnerable. Emails, social media accounts, financial applications, and private conversations all become accessible to an attacker who has successfully deployed spyware. For GCC students engaging in politically sensitive discussions or forming international academic networks, this level of monitoring poses serious risks to personal security.

Iranian actors have also employed traditional surveillance methods, such as compromising public Wi-Fi networks to execute man-in-the-middle attacks, intercepting unencrypted communications, and hijacking telephone lines. In one campaign, Iranian hackers reportedly gained access to Facebook accounts and telephone logs in addition to email communications. These methods allow attackers to construct detailed intelligence profiles on their targets, which can be used for future coercion.

Coercion and Blackmail

Once a target has been compromised, hostile state actors may escalate their tactics to blackmail or coerce compliance. Cyber units gather sensitive personal data, ranging from private conversations and social media interactions to personal photographs and financial information. Iranian operatives have previously exploited this information to threaten individuals with exposure unless they cooperate. This pressure may be used to

extract additional intelligence, compel changes in political stances, or force the target into recruitment efforts.

For some students, the mere knowledge that they are under surveillance can be enough to induce self-censorship. Those who fear potential repercussions from their home governments or academic institutions may alter their behaviour, avoid sensitive topics, or sever certain connections to minimise perceived risks. This psychological effect is a key objective of digital surveillance operations, allowing hostile actors to exert influence without direct intervention.

Iranian-linked cyber operations against GCC students in the UK reflect a highly strategic and multi-pronged approach, combining technical intrusions with social engineering to achieve long-term intelligence objectives. These methods are not deployed in isolation but often work in tandem—social media interactions that lead to phishing, phishing that installs malware, and malware that enables prolonged surveillance.

The overarching aim is to establish unauthorised access to a student's digital life, allowing for continued exploitation, intelligence gathering, and, where possible, coercion. Given the persistence of these threats, awareness and proactive cybersecurity measures are essential to mitigating the risks posed by state-backed cyber actors. Universities, policymakers, and security institutions must develop robust countermeasures to protect GCC students from becoming targets in an increasingly complex digital battlefield.

Role of Universities, Digital Platforms, and Mobile Communication

The cybersecurity risks faced by GCC students in the United Kingdom are significantly influenced by the environments in which they operate—universities, online platforms, and mobile communication networks. Each of these domains presents both vulnerabilities that adversarial actors can exploit and opportunities for mitigation through institutional policies and technological safeguards.

Universities as Targets and Defenders

Universities, as centres of intellectual exchange and open academic inquiry, represent attractive targets for cyber-espionage. Hostile state actors, particularly Iran, have previously targeted British universities in sophisticated cyber campaigns. In a notable 2018 incident, Iranian hackers established fraudulent university login portals to harvest credentials from British academic staff. By infiltrating university systems, adversarial cyber units could potentially access student directories, academic records, and institutional networks—information that could be exploited to identify and monitor GCC students of interest.

In addition to network intrusions, university infrastructure itself can inadvertently facilitate cyber risks. Many campuses provide public Wi-Fi networks and shared computer terminals, which, if inadequately secured, present opportunities for hostile actors to intercept communications or deploy malware. Iranian cyber units have been known to leverage such vulnerabilities to conduct credential theft and network surveillance operations.

Conversely, universities also serve as the first line of defence against state-sponsored cyber threats. Many UK institutions employ dedicated IT security teams that adhere to guidance from the National Cyber Security Centre (NCSC) to harden their systems against cyber intrusions. Measures such as network firewalls, intrusion detection systems, and multifactor authentication protocols enhance institutional resilience. Moreover, universities can play a proactive role in student cybersecurity education. Some institutions provide awareness seminars tailored to international students, informing them of phishing risks and best practices for secure digital behaviour.

Collaboration between universities, law enforcement agencies, and intelligence bodies further strengthens institutional defences. Some universities work closely with agencies such as MI5 and the NCSC to monitor and counter foreign intelligence activities on campus. However, the effectiveness of these measures varies across institutions. While some universities maintain rigorous security policies and cyber-awareness initiatives, others may lack the resources or urgency to address the growing threat posed by hostile cyber actors. Institutions that fail to adequately secure their networks risk not only exposing sensitive academic data but also unwittingly facilitating the targeting of their student populations.

Digital and Social Media Platforms as Vectors of Cyber Threats

Social media and online communication platforms represent a dual challenge in the cybersecurity landscape: they are among the most effective tools for adversarial actors to reach and manipulate students, yet they also provide mechanisms for defence and mitigation.

Social networking services, including Facebook, Twitter, LinkedIn, and Telegram, provide anonymity and an extensive reach for hostile operatives. Iranian cyber units have frequently created fraudulent social media profiles to engage with potential targets. A GCC student may be approached online by an individual posing as a fellow expatriate, a recruiter offering professional opportunities, or a journalist seeking insights on Middle Eastern affairs. These interactions often develop over time, with operatives carefully cultivating trust before introducing a phishing link or malware-laced document.

Mobile messaging applications such as WhatsApp, Telegram, and Signal are also primary channels for cyber intrusion. Iranian hackers have previously sent targeted phishing messages via WhatsApp, masquerading as conference organisers or research institutions. These messages contained links that directed recipients to malicious websites designed to steal login credentials. Additionally, social media activity itself can inadvertently provide attackers with intelligence. Students who publicly share personal

information, political views, or travel plans may unwittingly expose themselves to tailored cyber-espionage campaigns.

Despite these risks, major digital platforms have taken steps to counter state-sponsored cyber threats. Services such as Gmail, Facebook, and Twitter now employ artificial intelligence to detect suspicious login attempts and phishing activities. In some cases, Google has proactively alerted users—particularly academics and political activists—when their accounts were being targeted by state-backed actors. Certain platforms, such as LinkedIn, have also engaged in direct collaboration with cybersecurity researchers to identify and dismantle fraudulent profiles linked to espionage operations.

However, despite these mitigation efforts, determined state actors continue to exploit digital platforms effectively. The adaptability of adversarial cyber units ensures that new tactics emerge in response to platform countermeasures. As a result, GCC students must exercise heightened vigilance in their online interactions, carefully scrutinising unexpected messages, verifying the authenticity of contacts, and implementing strong security protocols, such as multifactor authentication.

Mobile Communication and Device Security

The pervasive reliance on mobile devices for communication, academic work, and financial transactions makes smartphones a critical vulnerability in the cybersecurity landscape. A successful compromise of a student's phone grants an adversary access to a vast repository of personal information, including call logs, private messages, and sensitive documents.

Hostile actors employ various techniques to exploit mobile communication channels. One common method involves SMS-based phishing, in which an attacker sends a seemingly legitimate text message containing a malicious link. Iranian cyber units have previously used this technique by distributing spyware disguised as VPN services or security updates. Once installed, this spyware enables the attacker to intercept calls, track real-time location, and extract encrypted messaging data.

Another concern is the continued use of home-country phone numbers while studying abroad. If a GCC student maintains their original SIM card while in the UK, they may remain subject to the surveillance infrastructure of their home government. In some cases, hostile intelligence services may seek to exploit existing surveillance mechanisms to monitor a target's communications. Additionally, if a student travels back to their home country during academic breaks, their communications may become vulnerable to interception by Iranian signals intelligence if routed through regions where Iran has operational influence.

Mobile application security is another pressing issue. Iranian cyber units have been linked to the development of malicious applications disguised as Islamic prayer apps, language-learning tools, or VPN services. Students who download unofficial or community-recommended applications risk exposing their devices to surveillance

malware. These programs can covertly activate microphones and cameras, collect keystrokes, and siphon off stored files.

Despite these threats, modern mobile operating systems offer increasingly robust security features. Apple's iOS and Google's Android both incorporate app verification systems that flag suspicious software and restrict access to sensitive device functions. Messaging applications such as WhatsApp and Signal employ end-to-end encryption, ensuring that intercepted communications remain unreadable to third parties—provided the device itself is not compromised. Universities and cybersecurity agencies also encourage students to adopt best practices, such as keeping their operating systems updated, using reputable security software, and enabling app permission restrictions to limit data exposure.

The security of GCC students in the UK is inherently linked to the policies and safeguards implemented across university networks, digital platforms, and mobile communication systems. A well-defended university infrastructure can detect and neutralise many initial cyber intrusion attempts, while proactive security measures by digital platforms can help identify and mitigate espionage campaigns. Students themselves play a crucial role in cybersecurity resilience by exercising caution in online interactions, avoiding the use of unverified applications, and maintaining strict security protocols on their mobile devices.

Ultimately, collaboration between universities, technology firms, and national cybersecurity agencies is essential in countering the persistent cyber threats posed by state actors. The National Cyber Security Centre has underscored the importance of securing higher education institutions against foreign cyber interference, issuing guidelines for both universities and students to mitigate state-sponsored espionage. Given the continued evolution of hostile cyber tactics, an adaptive and coordinated approach remains vital to ensuring the digital safety of GCC students studying in the United Kingdom.

Documented and Suspected Cases of Targeting

While cyber operations targeting GCC students are inherently covert, a series of documented incidents and investigative reports provide insight into the methods used by hostile state actors. These cases illustrate the tangible threats posed by state-backed cyber units and highlight the vulnerabilities that foreign students, particularly those from the Gulf region, face while studying in the UK.

Iranian Cyber-Espionage Targeting Middle East Experts in the UK (2021)

In 2021, cybersecurity firm Proofpoint uncovered an Iranian cyber operation in which the hacking group known as Charming Kitten (APT35) impersonated London-based university academics to target individuals engaged in Middle Eastern affairs. The attackers sent phishing emails purporting to be from scholars at SOAS University, inviting academics, journalists, and policy researchers to an event. To enhance credibility, the hackers even created a fraudulent webpage on a SOAS-affiliated website.

Victims who entered their login credentials into this platform unknowingly granted Iranian intelligence access to their email accounts, enabling the attackers to monitor correspondence and steal sensitive information. Security analysts have noted that Iran has long prioritised the targeting of academics, scientists, and diplomats in Western institutions as part of its broader intelligence-gathering efforts.

While this campaign explicitly focused on faculty and researchers, GCC students enrolled in political science, security studies, or international relations programmes could easily have been collateral victims, given their involvement in similar academic circles. The willingness of Iranian cyber units to exploit university infrastructure for espionage underscores the risk that UK-based Gulf students may face, particularly those engaging in politically sensitive discourse.

Thamar Reservoir: An Extensive Iranian Cyber Campaign (2014–2015)[7]

In 2015, the Israeli cybersecurity firm ClearSky uncovered an extensive Iranian cyber-espionage campaign known as “Thamar Reservoir,” which targeted approximately 500 individuals across the Middle East, with 44% of victims based in Saudi Arabia. The operation focused on high-profile figures, including retired military officers, security experts, journalists, and senior government officials. Among the documented targets were a finance minister of a Middle Eastern country and Qatar’s diplomatic mission in London.

The campaign relied on a combination of targeted phishing emails and malware to infiltrate victims’ computers and extract sensitive intelligence. Analysts concluded that the perpetrators were not engaged in financially motivated cybercrime but rather a long-term espionage effort aimed at infiltrating strategic networks and institutions.

While the available evidence does not explicitly confirm that GCC students in the UK were among the targets, the campaign’s focus on Gulf nationals, including those affiliated with diplomatic institutions in London, suggests that Iranian cyber units were

[7] ClearSky Cyber Security. *Thamar Reservoir: An Iranian Cyber-Attack Campaign Against the Middle East.* ClearSky Cyber Security, June 2015. https://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf.

actively seeking intelligence on Gulf-related activities in the UK. It is plausible that similar methods could have been used to target student organisations, particularly those linked to Saudi or Emirati diplomatic and academic circles.

Amnesty International and Human Rights Watch Expose APT42 (2022)[8]

In 2022, Amnesty International and Human Rights Watch identified an Iranian phishing campaign linked to the state-backed hacking unit APT42 (also associated with Charming Kitten). The investigation revealed that at least 18 high-profile individuals had been targeted, including a women's rights activist from a Gulf state. The attackers employed social engineering tactics, sending WhatsApp messages while posing as representatives of a Beirut-based think tank.

The targets were invited to an event and asked to RSVP via a link that redirected them to a fraudulent Google login page. Once the victims entered their credentials, attackers gained full access to their email accounts, cloud storage, and contact lists, allowing them to conduct a bulk data extraction.

The targeting of a Gulf-based activist highlights the direct interest Iranian cyber units have in individuals from GCC countries, particularly those involved in advocacy, political discourse, or human rights activism. Given that WhatsApp and other messaging platforms are commonly used by students, this case demonstrates how easily similar tactics could be deployed against GCC nationals studying in the UK. Even well-informed individuals fell victim to these sophisticated credential-harvesting schemes, underscoring the need for increased cybersecurity vigilance.

Recruitment of Foreign Students for Espionage: The German Case (2017–2019)

Between 2017 and 2019, German intelligence agencies investigated and ultimately arrested a 31-year-old Pakistani student accused of spying for Iran's Quds Force, a paramilitary unit of the Islamic Revolutionary Guard Corps (IRGC). The individual, who had entered Germany as an international student, was tasked with gathering intelligence on Jewish and Israeli institutions in Europe.

This case demonstrates that Iranian intelligence actively seeks to recruit foreign students studying abroad, leveraging their access to academic environments and social circles. While this particular incident involved surveillance of Jewish communities, the same recruitment model could be applied to GCC students, particularly those from Bahrain or Saudi Arabia. Given Iran's geopolitical interests, it is conceivable that Iranian intelligence operatives would seek to cultivate Gulf nationals, either for ideological indoctrination or coercive intelligence-gathering efforts.

---

[8] Human Rights Watch. "Iran: State-Backed Hacking of Activists, Journalists, and Politicians." *Human Rights Watch*, December 5, 2022. https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians.

A foreign student recruited for such purposes could be directed to monitor dissident communities, provide insights into Gulf diplomatic initiatives, or even install malware on university networks. The precedent established by the German case suggests that similar recruitment attempts may occur elsewhere in Europe, including the UK.

Leaked Iranian Strategy to Leverage Foreign Students (2023)[9]

In late 2023, an Iranian dissident group leaked an audio recording of a senior Iranian official, Hamid Reza Haddadpour, detailing a strategic initiative to cultivate foreign students as intelligence assets. The official described international students as "intellectual footholds" for the regime, explicitly referencing the long-term goal of influencing future decision-makers abroad. He noted that many of these students were "the children of influential individuals from their own countries" and would eventually inherit political or economic leadership roles.

The recording revealed a directive from Iran's Supreme Leader to discreetly establish connections with international students, particularly those studying in Iran. The plan involved appointing cultural advisors to engage with these students while avoiding terms such as "missionary" or "mentor" to prevent suspicion.

Although this initiative primarily focused on students studying within Iran, it offers critical insight into Tehran's broader approach to leveraging young foreigners as long-term assets. The fact that Iranian officials view foreign students as potential intelligence resources raises concerns that similar efforts could be directed at GCC students studying abroad, particularly in the UK.

One particularly concerning revelation was the claim that an Islamic college in the UK, allegedly affiliated with an Iranian university, was involved in regime-linked activities. While the institution denied the allegations, the report highlighted the existence of Iranian soft-power networks operating within British academia.

These documented incidents collectively illustrate the range of methods employed by Iranian intelligence and cyber units to target Gulf-related individuals, including students, diplomats, and academics. The combination of technical hacking campaigns, credential harvesting, espionage, and direct recruitment efforts underscores the multifaceted nature of the threat.

While not every GCC student in the UK will be targeted, those with political or security-related affiliations, as well as those from influential families, face heightened risks. Moreover, even students with no direct political involvement can become collateral targets in broad phishing campaigns or be identified as future assets due to their academic trajectory.

---

[9] Iran Focus. "Leaked Audio File Reveals Tehran's Plan to Recruit Foreign Students." *Iran Focus*, January 26, 2024. https://iranfocus.com/intelligence-reports/50258-leaked-audio-file-reveals-tehrans-plan-to-recruit-foreign-students/.

These cases underscore the necessity for robust cybersecurity awareness and institutional safeguards. The reality is clear: Iranian cyber operations are not theoretical threats but ongoing campaigns that have already penetrated Western academia. The UK must take this issue seriously, ensuring that students, universities, and government agencies are fully equipped to counter such threats and prevent hostile intelligence services from exploiting British academic institutions as a battleground for espionage and cyber warfare.

Geopolitical Motivations and Long-Term Consequences

Strategic Motivations

The systematic targeting of GCC students by hostile state actors, particularly Iran, is not merely a matter of opportunistic cyber intrusion but a calculated component of Tehran's broader geopolitical strategy. The long-standing rivalry between Iran and the Gulf states—primarily Saudi Arabia and the UAE—has been described as a regional cold war, driven by competing ideological, political, and security interests. While Qatar has maintained relatively cordial ties with Iran, the rest of the GCC remains firmly opposed to Tehran's regional ambitions. Iranian intelligence views GCC nationals as valuable sources of intelligence and influence for several key reasons.

One of the primary objectives of Iranian cyber operations is the collection of intelligence on rival Gulf states. Students from the GCC, particularly those from prominent families, often maintain strong ties to political, business, and security circles back home. Their personal communications, emails, and social media interactions can provide adversarial intelligence agencies with insights into elite opinions, policy discussions, and internal dynamics within Gulf states.

A successful compromise of a student's device can yield contact lists, private correspondence, and personal data that feed into Iran's broader intelligence apparatus. Iranian hackers have previously demonstrated their focus on Saudi and Emirati targets, conducting sophisticated phishing campaigns to infiltrate their digital networks. These operations are not financially motivated but designed to serve national security interests by monitoring perceived adversaries.

Beyond intelligence collection, Iran seeks to exert ideological influence over young Gulf nationals. Many GCC students studying abroad are exposed to diverse perspectives and greater personal freedoms, creating an opportunity for Iranian operatives to cultivate sympathisers. This can occur through direct engagement—such as recruitment attempts at cultural or academic events—or through the dissemination of tailored narratives on digital platforms.

By leveraging online propaganda, social media discourse, and targeted interactions, Iran can attempt to shape the worldviews of GCC students, particularly those who may already hold grievances against their home governments. A leaked audio recording from an Iranian government official detailed a strategy to turn foreign students into long-term advocates for the Islamic Republic, describing them as "intellectual footholds" in their respective countries. This soft power approach seeks to create a network of future influencers who can act as informal amplifiers of Iranian-aligned narratives.

Recruitment of Assets

While ideological influence is one goal, Iranian intelligence agencies also seek to recruit foreign students as active assets. A student targeted during their university years may eventually ascend to a position of influence in government, security, or business, providing Iran with a long-term source of intelligence and operational leverage. Iranian officials have explicitly recognised this reality, noting that "many of these students will naturally take the place of their fathers" in positions of power upon their return home.

Recruitment efforts may take different forms. In some cases, students are cultivated over time through ideological persuasion, financial incentives, or promises of professional advancement. Others may be coerced through blackmail, particularly if Iranian intelligence has acquired compromising material through cyber intrusion. Shia students from Bahrain or Saudi Arabia may be viewed as particularly promising recruits, given Iran’s historical efforts to foster Shia opposition movements in the Gulf.

The case of a Pakistani student recruited in Germany to spy for Iran’s Quds Force illustrates this approach. The individual was tasked with conducting surveillance on Jewish and Israeli institutions in Europe, demonstrating how Iranian intelligence actively seeks to embed operatives in foreign academic environments. The same recruitment model could be applied to GCC students, particularly those in fields of strategic interest such as cybersecurity, energy policy, or nuclear studies.

Iran’s targeting of GCC students serves a broader strategic function by undermining Gulf security from within. By infiltrating the digital and personal networks of Saudi and Emirati nationals, Iranian intelligence can disrupt internal cohesion, fuel suspicions within Gulf governments, and create avenues for future subversion. This aligns with Tehran’s long-standing strategy of projecting power beyond its borders, not just through military interventions in Syria, Iraq, and Yemen, but also through cyber and intelligence operations targeting rival states.

The intelligence gained from GCC students may also have implications for Iran’s engagement with Western powers. The Gulf states maintain close security partnerships with the UK and the US, and any insights into these relationships—whether from students studying in the UK or involved in Gulf-UK business or diplomatic projects—could provide Iran with a strategic advantage. By monitoring Gulf nationals abroad, Tehran may be able to glean intelligence on key economic and security discussions involving its adversaries.

Long-Term Consequences

The ramifications of these cyber and intelligence operations extend beyond the immediate risks to individual students, impacting national security, diplomatic relations, and the integrity of academic environments.

Personal Risks for Students

For the individuals targeted, the consequences can be severe. Those who fall victim to cyber intrusions may have their personal data compromised, exposing sensitive communications, private photographs, and financial details to hostile intelligence services. In cases where blackmail is involved, students may be subjected to coercion, forced to act against their interests, or pressured into providing information on their peers.

Even students who are not directly compromised may experience the chilling effects of surveillance. The mere knowledge that Iranian cyber units actively target Gulf nationals may lead to self-censorship, with students refraining from political discussions or avoiding certain academic topics out of fear of being monitored. This not only undermines their educational experience but also creates an atmosphere of mistrust within student communities.

Threats to GCC National Security

The long-term security implications for the Gulf states are significant. If Iranian intelligence successfully recruits or compromises GCC nationals, it could result in security breaches at the highest levels of government and industry. A student who returns to Saudi Arabia or the UAE and later assumes a senior government or corporate role may unwittingly serve as a conduit for Iranian intelligence, providing Tehran with access to classified information or influencing policy decisions.

Even absent direct recruitment, the large-scale compromise of Gulf nationals' digital communications could provide Iran with an intelligence advantage. By monitoring the communications of hundreds of Saudi or Emirati students over several years, Iranian intelligence could map out key networks, identify future political figures, and track internal developments within the Gulf states. This level of insight could be used to Iran's advantage in diplomatic negotiations, proxy conflicts, or economic competition.

Diplomatic and Geopolitical Fallout

The exposure of Iranian cyber operations against GCC students in the UK could lead to diplomatic crises between the involved nations. The UK has previously called out Iran for state-sponsored cyber activities, and a sustained campaign against foreign students could result in retaliatory measures, including the expulsion of Iranian diplomats or sanctions on Iranian entities involved in cyber-espionage.

For the GCC states, the revelation of Iranian intelligence activities targeting their citizens abroad could further escalate tensions, leading to increased scrutiny of Iranian-linked institutions and individuals within the Gulf. This could contribute to a broader cycle of retaliation, with Gulf states potentially seeking to counter Iranian influence through their own intelligence measures.

Erosion of Academic Freedom and Security

One of the more insidious consequences of these cyber operations is the potential securitisation of academic spaces. Universities are meant to be centres of open discourse and intellectual exchange, but the persistent threat of espionage may lead to increased surveillance and restrictions on student activities.

GCC students may find themselves subject to heightened scrutiny, both from UK authorities and from their own governments, as concerns about foreign interference grow. This could result in restrictions on access to academic resources, increased monitoring of student associations, and a general climate of suspicion that undermines the academic experience.

At the same time, Iranian efforts to influence student communities could stifle open debate, with Gulf students feeling pressured to avoid politically sensitive discussions for fear of surveillance or retribution. This erosion of trust within academic institutions is a subtle but profound consequence of state-sponsored cyber-espionage.

The geopolitical motivations behind Iran’s targeting of GCC students are clear: espionage, influence, recruitment, and power projection. These operations are not isolated incidents but part of a broader intelligence strategy that has long been a pillar of Iranian foreign policy. If left unchecked, such activities could have severe long-term repercussions, compromising the security of Gulf states, undermining academic integrity, and fueling diplomatic tensions.

Recognising the scale and scope of this threat underscores the urgent need for proactive mitigation strategies. Universities, governments, and security agencies must work together to strengthen digital resilience, educate students on cybersecurity risks, and prevent hostile intelligence services from exploiting British academic institutions as battlegrounds for espionage and ideological warfare.

Mitigation Strategies

Countering the cybersecurity threats faced by GCC students in the UK requires a multi-tiered defence strategy that involves individuals, educational institutions, and national security agencies. While students must adopt robust cyber hygiene to protect themselves against digital intrusion, universities play a pivotal role in securing their networks and providing clear response mechanisms. At the governmental level,

intelligence-sharing, legal deterrence, and diplomatic action are essential to disrupting state-backed espionage efforts.

This section outlines a three-pillar mitigation approach, ensuring that GCC students can pursue their academic ambitions without the persistent threat of cyber-espionage, coercion, or ideological manipulation.

Strengthening Individual Cyber Hygiene: Best Practices for GCC Students

GCC students can significantly reduce their risk of being targeted by hostile cyber actors by implementing rigorous digital security measures. Key steps include:

Be Wary of Unsolicited Communications

Students should treat unexpected emails, messages, or phone calls with a high degree of skepticism—especially those prompting them to click a link, download an attachment, or share personal information. Iranian cyber units are known to craft highly convincing phishing attempts, often mimicking legitimate university communications, conference invitations, or official-looking password reset requests.

- **Verification Protocol:** Any request that appears unusual should be verified through official channels (e.g., directly contacting university IT departments) rather than engaging with the sender.
- **Government Guidance:** The UK's National Cyber Security Centre (NCSC) has advised high-risk individuals to be especially cautious of unsolicited contact and phishing tactics.

Secure All Online Accounts with Strong Authentication

- Use strong, unique passwords for email, banking, and social media accounts.
- Enable two-factor authentication (2FA) to add an additional layer of security. Avoid SMS-based 2FA, as attackers can hijack phone numbers through SIM-swapping attacks.
- Use an authentication app (such as Google Authenticator) or a hardware security key to prevent unauthorized access.

Regularly Update Devices & Install Cyber Defences

- Enable automatic software updates on all devices to patch vulnerabilities.
- Install trusted antivirus and anti-malware software to detect and neutralize cyber threats.
- Avoid jailbreaking or rooting phones, as this disables key security protections and makes devices vulnerable to spyware.

Practise Safe Digital & Mobile Communications

- Avoid logging into sensitive accounts on public Wi-Fi networks unless using a trusted VPN. University-provided encrypted networks, such as Eduroam, are preferable.
- Be cautious with USB drives—state-backed cyber actors have been known to distribute infected USB sticks at academic events.
- Use end-to-end encrypted messaging apps, such as Signal or WhatsApp, but remain aware that if a device is compromised, even encrypted conversations can be intercepted.
- Consider using disappearing messages for sensitive conversations to minimize long-term data exposure.

Limit Social Media Exposure & Digital Footprint

- Tighten privacy settings on social media to restrict who can view personal information, friends lists, and past posts.
- Avoid sharing real-time locations or travel plans that could be exploited by hostile actors.
- Use pseudonyms or nicknames on online forums where nationality could make individuals a target.

Monitor for Signs of Compromise

Students should regularly check for unusual activity, such as:

- Unexpected password reset emails.
- Suspicious messages sent from their account without their knowledge.
- Unexplained battery drain, which could indicate spyware running in the background.
- New apps installed without their permission.

If anything appears suspicious, immediately report it to university IT security teams or cybersecurity professionals.

Institutional Responsibility: Securing Universities and Student Networks

UK universities hosting GCC students must proactively safeguard their digital environments against state-sponsored cyber intrusions. Institutions should implement the following security measures:

Cybersecurity Awareness Training for International Students

- Mandatory cybersecurity training should be incorporated into student orientations, focusing on practical defences against phishing and cyber espionage.
- Universities should partner with the NCSC and cybersecurity firms to offer tailored guidance on protecting high-risk individuals from state-sponsored cyber operations.

Strengthening Campus Network Security

- Implement WPA2/WPA3 encryption for university Wi-Fi networks and require strong authentication for access.
- Monitor for suspicious data transfers from student accounts—anomalous traffic spikes may indicate a compromise.
- Regularly patch and update university websites, portals, and databases to prevent exploitation by hostile actors.
- Deploy intrusion detection systems that flag unusual patterns, such as repeated failed login attempts from foreign locations.

Establish Clear Incident Reporting Channels

- Universities should provide a dedicated cybersecurity contact point for students to report suspected cyber threats.
- If state-sponsored activity is suspected, institutions must coordinate with UK authorities, including the NCSC and MI5.

Protecting Student Data from Exploitation

- Restrict public access to student directories that list names, nationalities, or email addresses—these can serve as reconnaissance tools for hostile actors.
- Provide high-risk students access to advanced security protections, such as Google’s Advanced Protection Program, to mitigate targeted phishing attempts.

Vigilance Against Foreign Espionage on Campus

- University staff and security teams should remain alert to foreign intelligence operatives infiltrating student networks, particularly through political science and security studies programs.
- Any suspicious engagement by visiting researchers, journalists, or "recruiters" should be flagged and, if necessary, escalated to UK intelligence agencies.

Government Action: Strengthening National Security Measures

The UK and GCC governments have a shared responsibility to protect students from state-sponsored cyber threats. Key actions include:

Enhancing UK Cyber Defences & Counter-Espionage Laws

- The UK must continue to publicly expose state-backed cyber threats, as seen in joint advisories by the NCSC, FBI, and allies.
- UK authorities should conduct targeted cybersecurity briefings for universities and at-risk student groups.
- Strengthening counter-espionage laws to criminalize cyber-enabled spying on students is essential. Foreign operatives caught engaging in harassment or recruitment efforts should be prosecuted or expelled.

GCC Governments: Preemptive Action to Protect Students

- GCC states should equip students with pre-departure cybersecurity training, ensuring they understand digital risks before studying abroad.
- Embassies in the UK should establish dedicated cybersecurity support teams, providing students with rapid-response mechanisms for reporting suspected cyber harassment.
- Coordination with UK authorities should be expanded, allowing intelligence-sharing on Iranian cyber tactics and emerging threats.

International Collaboration & Intelligence Sharing

- The UK should develop a centralized reporting mechanism for foreign cyber threats targeting academic institutions.
- GCC states should increase collaboration with cybersecurity firms and Western intelligence agencies to track and dismantle cyber operations targeting their citizens.

Monitoring & Disrupting Hostile Cyber Infrastructure

- Cybersecurity agencies should identify and block phishing domains, malware servers, and surveillance tools used in cyber operations against students.
- UK telecom providers should detect and prevent SMS phishing campaigns targeting GCC nationals studying abroad.
- Diplomatic pressure should be applied against states engaged in cyber-espionage on UK soil, with the potential for sanctions or diplomatic expulsions.

A Multi-Layered Defence Against Foreign Cyber Threats

The security of GCC students in the UK cannot be left to individual vigilance alone. A coordinated strategy—combining personal cybersecurity awareness, university security measures, and governmental counter-espionage efforts—is essential.

By implementing these measures, universities can remain places of learning and academic freedom, free from foreign interference. At the same time, UK and GCC authorities can ensure that young Gulf nationals—many of whom will become future leaders—are not compromised, manipulated, or coerced by hostile intelligence agencies.

The challenge is significant, but through proactive defence, strategic collaboration, and institutional vigilance, the UK can mitigate the risks posed by state-backed cyber threats, safeguarding both its students and its academic institutions.

Government Action: Strengthening National Security Measures

Both UK and GCC governments play critical roles in safeguarding students against cyber and espionage threats.

British authorities should continue public exposure of state-backed cyber threats, as seen in joint advisories by the NCSC and allied agencies. Increasing engagement with universities to provide intelligence briefings on foreign interference risks is essential. Law enforcement agencies, including MI5 and GCHQ, should proactively inform at-risk student groups and implement countermeasures against espionage.

On the legislative front, the UK is in the process of strengthening counter-espionage laws. Ensuring that these statutes address cyber-enabled spying on students is crucial. Any operatives found engaging in harassment or recruitment efforts should be prosecuted or expelled under malign foreign interference laws.

GCC states should equip their students with pre-departure cybersecurity training, ensuring that they understand the risks they may face while studying abroad. Embassies in the UK should provide dedicated cybersecurity support for students, offering them a reporting mechanism for suspected cyber harassment.

GCC governments should coordinate with UK authorities on intelligence-sharing, particularly regarding known Iranian cyber tactics. However, they must balance security concerns with the need to avoid excessive surveillance of their own citizens, which could inadvertently drive some students toward adversarial influence.

The UK should enhance cooperation between universities, security agencies, and international partners to develop a centralized reporting mechanism for foreign cyber threats targeting academic institutions. Cybersecurity initiatives should focus on monitoring and blocking attacker infrastructure, such as phishing domains and malware command-and-control servers.

A multi-pronged approach—combining individual vigilance, institutional security, and governmental oversight—is necessary to mitigate the cyber risks faced by GCC students in the UK. While no single measure can eliminate the threat, a well-informed student body, fortified university systems, and robust national security measures can significantly reduce the effectiveness of foreign espionage efforts.

By adopting a proactive stance, UK and GCC authorities can ensure that educational institutions remain places of learning and collaboration, free from the covert influence of hostile intelligence operations. The ultimate goal is to create an environment in which GCC students can pursue their studies without fear of digital surveillance, manipulation, or coercion, reinforcing both academic integrity and national security.

Conclusion

GCC students pursuing higher education in the UK find themselves at a unique crossroads—where academic aspirations intersect with the geopolitical ambitions of hostile state actors. Their digital lives, personal networks, and even future career trajectories make them attractive targets for espionage, with Iran leading efforts to exploit their online presence, social circles, and communications. This risk assessment has detailed the various mechanisms employed—phishing, malware, and social engineering—and demonstrated how both universities and digital platforms serve as contested spaces where foreign intelligence agencies seek to exert influence.

The evidence is clear: Iranian cyber-espionage operations have already penetrated British academia, targeting scholars, activists, and Middle Eastern nationals. Given Iran's established interest in Gulf affairs, it is reasonable to conclude that GCC students studying in the UK are not exempt from these activities. The motivations behind such operations range from intelligence gathering and ideological influence to long-term recruitment—each serving Tehran's broader strategic competition with the Gulf states.

However, these threats are not insurmountable. By cultivating awareness and adopting proactive security measures, GCC students can substantially reduce their exposure to cyber intrusion. A well-informed student body—one that understands the nature of phishing campaigns, digital surveillance, and recruitment tactics—can deny hostile actors the access they seek. Universities, as custodians of knowledge and safety, have a responsibility to strengthen cybersecurity infrastructure, educate students on digital threats, and ensure that academic institutions remain places of learning rather than sites of covert intelligence activity.

At the national and international level, coordinated vigilance is imperative. Information-sharing between governments, universities, and cybersecurity agencies can help detect and neutralize espionage efforts before they take root. Strategic deterrence—whether through diplomatic pressure, legal accountability, or cyber countermeasures—can make it increasingly costly for malign actors to conduct such operations on British soil.

Protecting GCC students is not merely a matter of safeguarding individuals—it is about preserving the integrity of international education, ensuring academic freedom, and preventing foreign regimes from manipulating or coercing young Gulf nationals. These students represent the future leadership, industry, and governance of their respective countries. Allowing them to study abroad without the specter of digital surveillance and interference is essential not only for their personal security but for the long-term stability and independence of the Gulf region itself.

The international academic environment should be a place of intellectual exchange, not a battleground for foreign intelligence operations. If left unchecked, the continued targeting of GCC students by hostile cyber actors will have long-term consequences—not just for personal security, but for national resilience and international education. The UK and GCC nations must prioritize student cybersecurity through intelligence-sharing, campus-level protections, and legal countermeasures to deter malign actors. Without decisive action, students will remain vulnerable to digital intrusion and coercion, reinforcing Iran’s ability to manipulate and monitor the Gulf’s future leaders. The time to act is now.