OFFENSIVE CYBER OPERATIONS ABROAD INFLUENCE US CONGRESSIONAL LEGISLATION

By Lori Cole – ISSA member Blue Ridge and Triad of NC Chapters
and Kory Fear – ISSA member Triad of NC Chapter

Recent offensive cyber operations conducted in the Middle East have prompted US congressional legislative reform. Electronic warfare conducted by United Arab Emirates sponsored cyber group Project Raven against journalists and human rights activists has served as a catalyst for the enactment of an amended 2020 National Defense Authorization Act, which aims to curb similar activity in the future.

As reported by *Reuters* in January 2019, Project Raven was operating as a clandestine team of offensive cyber operatives that were recruited to assist the United Arab Emirate (UAE) monarchy in conducting surveillance operations against intelligence targets, including foreign governments and military, domestic dissidents, and human rights activists [3]. Project Raven was staffed by former US government cybersecurity analysts and operators, trained by America's experts on electronic warfare, the National Security Agency and the Central Intelligence Agency.

Project Raven was a compartmentalized hacking group of the UAE National Electronic Security Agency (NESA), essentially an NSA equivalent, directed by the Ministry of Interior. According to *Reuter's* investigative reporting [2], NESA intelligence objectives included gaining initial electronic access and acquiring digital surveillance of a variety of targets: investigative reporters, UAE dissidents, neighboring state government officials, the Muslim Brotherhood, Hezbollah, and ISIS—without regard to target citizenship status. For example, all of the following could be considered valid targets for offensive hacking campaigns carried out by Project Raven: a British journalist, an Emirati teenager, a child in the household of a person of intelligence value, or an American citizen. Foreign intelligence objectives differ from American intelligence objectives, and so does the target scope. But should American cyber operatives target American citizens in support of these efforts? What does US law dictate?

Former American intelligence operatives are not prohibited from sharing generic spycraft and there are no specific laws that prevent hackers from participating in foreign cyber operations. There are clear laws, however, that make hacking US networks and citizens illegal. This gray intersection of hacking and immunity has served as a catalyst for Congressional legislative change in the United States, prompted by Project Raven. Exposure of Project Raven by mainstream media channels (e.g., *Reuters, New York Times*) raised the concern

of former US intelligence operatives becoming key players in foreign cyber wars and the ethics of targeting Americans at the direction of those governments.

The dark matters involving Project Raven were revealed by a whistle-blower who left the Emirati offensive cyber security program in May 2017 [2]. The former Raven operative resigned due to ethical disagreements with Project Raven directives, specifically, orders to hack US citizens to acquire intelligence. This ethical conflict highlights the larger need for legal boundaries surrounding acts of cyber espionage involving former intelligence agents and potentially civilian security professionals.

National Defense Authorization Act

The National Defense Authorization Act (NDAA) is the primary way that Congress executes its Constitutional duties to ensure military readiness and to implement national defense strategies to confront global threats [10]. The NDAA also strengthens the Congressional oversight of US cyber operations and enhances the Department of Defense's cybersecurity strategy and cyber warfare capabilities.

The 2020 NDAA Amendment

As a result of the exposure of Project Raven, amendments to the 2020 NDAA were agreed to and enacted. Specifically, there was an amendment to title VII of H.R. 3494, entitled, "Reports and Other Matters" [6]. It was recorded in the Congressional Record of the House, July 2019 [4] that intelligence operations are imperative to the security of the United States and the concern of former intelligence professionals serving foreign governments is undeniable. The Record of the House reflected direct citation of former NSA operatives employed by Project Raven in the United Arab Emirates, who had conducted offensive cyber operations and utilized surveillance techniques to assist in the Arab monarchy's intelligence mission, specifically the targeting of multiple US citizens in 2017. The UAE's intelligence operations included surveillance and electronic targeting of terrorists, human rights activists, and journalists. The concern is that US intelligence agency-trained personnel advising and participating in cyber operations for foreign governments may go against coveted American ideals such as the First Amendment if used against US citizens.

Exposure of Project Raven…raised the concern of former US intelligence operatives becoming key players in foreign cyber wars and the ethics of targeting Americans at the direction of those governments.

The 2020 NDAA amendment to title VII will enable better understanding of the nature, impact, and security implications of former US intelligence professionals who serve foreign governments or participate in foreign cyber operations. This provision was signed into law and will require that the intelligence community provide Congress with an annual assessment of risks to national security posed by former intelligence operatives. It requires the Director of National Intelligence, in coordination with other intelligence community partners, to conduct an annual assessment of the homeland security vulnerabilities associated with former intelligence community employees providing intelligence assistance to a foreign government.

Pertinent text of the amendment is as follows:

> "SEC. 720. ASSESSMENT OF HOMELAND SECURITY VULNERABILITIES ASSOCIATED WITH CERTAIN RETIRED AND FORMER PERSONNEL OF THE INTELLIGENCE COMMUNITY.

> (a) ASSESSMENT REQUIRED. —Not later than the date that is 120 days after submission of the report required under section 704 of this Act, and annually thereafter, the Director of National Intelligence, in coordination with the Under Secretary of Homeland Security for Intelligence and Analysis, the Director of the Federal Bureau of Investigation, the Director of the Central Intelligence Agency, and the Director of the Defense Counterintelligence and Security Agency, shall submit to the appropriate congressional committees an assessment of the homeland security vulnerabilities associated with retired and former personnel of intelligence community providing covered intelligence assistance." [6]

This new measure will allow Congress to re-examine the effectiveness of current US laws, policies, procedures, and other restrictions on former intelligence operatives to prevent "covered intelligence assistance" without prior authorization. Specifically, this risk will be assessed by investigating and reporting on former members of the intelligence community who directly or indirectly assist a foreign government through a company or other entity relating to intelligence or law enforcement activity. This also includes operations that abuse human rights, violate US law, or infringe on the privacy of US citizens (e.g., surveillance).

Potential vulnerabilities could result from the prescribed investigations. For example, if a former NSA offensive operator who specialized in initial access into Chinese government networks left the Agency and became a private cybersecurity contractor in Hong Kong, the application of prior intimate technical knowledge (of access methods or evasive techniques) would be a likely risk, making this former operative even more effective.

Moving forward this amendment will most likely result in professional (and potential geographic) restrictions to new and current members of the US intelligence community, not unlike a non-compete clause that many businesses use to prevent an employed party from entering into a relationship with a direct competitor.

While this may discourage some applicants from joining the US intelligence community, this could also reduce the transfer of US intelligence tactics and techniques being used by foreign governments. The International Transfer in Arms Regulations (ITAR) are export controls designed to ensure that defense-related technology does not transfer into enemy hands, encompassing a variety of items from missile technology to significant military equipment. ITAR regulations also cover cyber tradecraft as it is considered technical data directly related to defense services. The ITAR mandates that access to these sensitive materials be restricted to US citizens only [9].

Will it prevent hacking of US persons in the future?

While the 2020 NDAA amendment will not prevent the hacking of US persons, it should serve to restrict former US intelligence operatives from aiding or participating in foreign electronic warfare that may target American citizens without proper authorization. More immediately, the amendment will promote the acknowledgment and handling of operative risk. Exploring and understanding the capabilities of Agency-trained personnel, and the potential threat they may pose if those skills were utilized against the United States, will serve as a new measure of risk in cyber warfare.

The amendment raises several questions:

- Would increased monitoring of former US Intelligence members encroach on their privacy rights?
- Will the risk assessment of former US intelligence members be adequate to inform counter intelligence measures?
- How effective will future restrictions be in mitigating assisted espionage, short of changing federal law?

What is clear from the amendment is that the US government is taking an initial step in addressing the risk of former US intelligence operatives working on behalf of foreign governments. Identifying and understanding this risk will inform future intelligence and homeland security policies that shape the defensive posture throughout America. This new law will require US government agencies (e.g., FBI, NSA) to report the risk associated with former operative activities, which could drive US counterintelligence strategy.

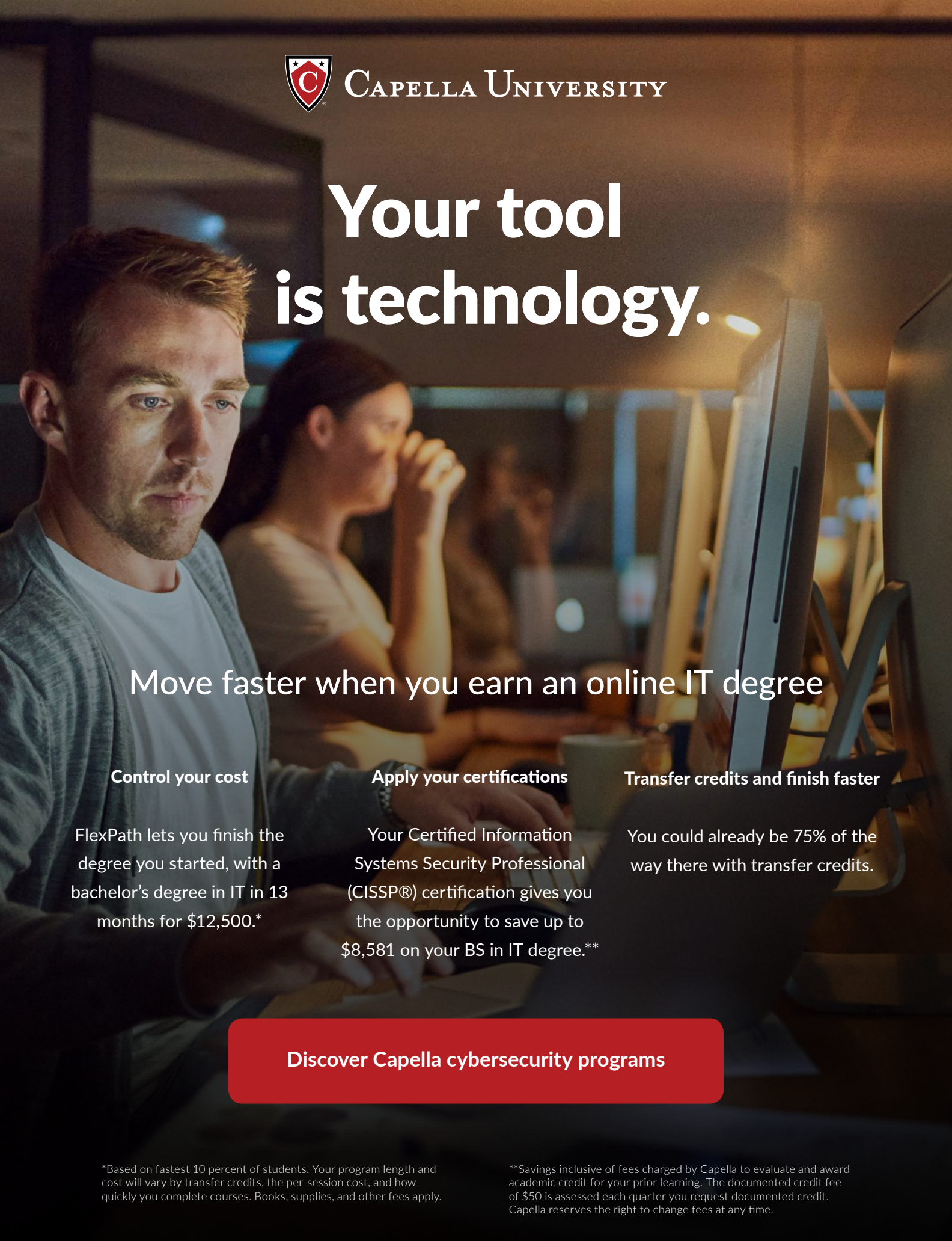
Beyond the intelligence community, security professionals should consider the laws that govern cybersecurity practices, such as:

- the Computer Fraud and Abuse Act (CFAA), which covers a broad range of cyber conduct, including hacking (intentionally accessing a computer without authorization) [7]
- the Federal Information Security and Management Act (FISMA), a US federal law that requires federal agencies to develop and implement an information security and protection program [5]
- the Arms Export Control Act [1], which prohibits unlicensed export of "defense services" detailed in the International Traffic in Arms Regulations (ITAR) [9] and US Munitions List (USML) [8], which includes intelligence tradecraft (Category XVII: Classified Articles, Technical Data and Defense Services Not Otherwise Enumerated)

Security professionals should consider these laws as they prescribe the boundaries of offensive cyber behavior, detail the need for cyber defense and strategy, and define legal conduct in the context of cybersecurity.

Conclusion

Federal cyber legislation will continue to evolve; the challenge for government agencies and current and former employees will be understanding applicable laws and acting in accordance with those laws. As the laws of security conduct translate into cyberspace, they will affect practitioners globally. The exposure of cyber operations conducted by Project Raven escalated the rules of engagement to the US legislative forefront prompting change.



Capella University

Your tool is technology.

Move faster when you earn an online IT degree

Control your cost

FlexPath lets you finish the degree you started, with a bachelor's degree in IT in 13 months for $12,500.*

Apply your certifications

Your Certified Information Systems Security Professional (CISSP®) certification gives you the opportunity to save up to $8,581 on your BS in IT degree.**

Transfer credits and finish faster

You could already be 75% of the way there with transfer credits.

Discover Capella cybersecurity programs

*Based on fastest 10 percent of students. Your program length and cost will vary by transfer credits, the per-session cost, and how quickly you complete courses. Books, supplies, and other fees apply.

**Savings inclusive of fees charged by Capella to evaluate and award academic credit for your prior learning. The documented credit fee of $50 is assessed each quarter you request documented credit. Capella reserves the right to change fees at any time.

The 2020 NDAA amendment to title VII, requiring the intelligence community to assess the security risk of former operatives working on behalf of foreign governments, continues the conversation surrounding safeguarding cybersecurity tradecraft as intellectual capital. This sets a precedence of actively responding to risks to national security posed by former intelligence operatives and will hopefully prevent "covered intelligence assistance" without prior authorization.

References

1. Arms Export Control Act. (Aug 13, 2018) - https://legcounsel.house.gov/Comps/Arms%20Export%20Control%20Act.pdf.
2. Bing, Christopher and Joel Schectman. "American Hackers Helped UAE Spy on Al Jazeera Chairman, BBC Host," Reuters Investigates April 1, 2019 - https://www.reuters.com/investigates/special-report/usa-raven-media/.
3. Bing, Christopher and Joel Schectman. "Inside the UAE's Secret Hacking Team of American Mercenaries," Reuters Investigates (Jan 30, 2019) - https://www.reuters.com/investigates/special-report/usa-spying-raven/.
4. "Congressional Record of the House" NDAA and Project Raven (July 16, 2019) - https://www.congress.gov/116/crec/2019/07/16/CREC-2019-07-16-pt1-PgH5858.pdf.
5. DHS CISA, "Federal Information Security and Management Act of 2014," Department of Homeland Security - https://www.cisa.gov/federal-information-security-modernization-act.
6. H.R.3494 - Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Congress.gov - https://www.congress.gov/bill/116th-congress/house-bill/3494/text#toc-HE03B575343AF4B138EA95FF37A9E1239.
7. Eltringham, S. Editor in Chief. "Prosecuting Computer Crimes. Computer Fraud and Abuse Act," Department of Justice (1986) - https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.
8. "United States Munitions List," Electronic Code of Federal Regulations (2020) - https://www.ecfr.gov/cgi-bin/text-idx?SID=86008bdffd1fb2e79cc5df41a180750a&node=22:1.0.1.13.58&rgn=div5#se22.1.121_11.
9. US Department of State, "The International Traffic in Arms Regulations," Directorate of Defense Trade Controls - https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987.
10. US Senate Committee on Armed Services, "FY2020 NDAA Summary" - https://www.armed-services.senate.gov/imo/media/doc/FY20%20NDAA%20Conference%20Summary%20_%20FINAL.pdf.

About the Authors

Lori Cole, GSEC, GCIH, is a security operations manager at Hanesbrands Inc., a member of the Women in Engineering and Cybersecurity Communities of the IEEE, and the CompTIA Advancing Women in Technology Group. She can be reached at LoriSaysRAWR@gmail.com.

Kory Fear, Network+, is a security analyst II at Hanesbrands Inc., a member of the ISSA Triad Chapter, and can be reached at Sec.Fear@outlook.com.