DEVELOPING THE "HACK-ALONG": OVERCOMING EXPERIENTIAL OBSTACLES FOR CYBERSECURITY STUDENTS IN HOMELAND SECURITY PROGRAMS

CHRISTOPHER WHYTE, Virginia Commonwealth University
cewhyte@vcu.edu

ABSTRACT

Cybersecurity remains one of the most challenging subjects to develop accessible curricula for students in homeland security, emergency preparedness, and security-oriented degree programs. This article describes the development of a unique experiential learning opportunity that helps students overcome one of the most challenging learning objectives in such coursework: the conceptualization of sophisticated cyber operations. The *hack-along* is a simulated cyber operation exercise. Cyber experts guide students through multiple scenarios highlighting attacker and defender perspectives. Students ask detailed questions and discuss operational planning and decision-making strategies resulting in higher levels of student content engagement.

INTRODUCTION

Students in homeland security and emergency preparedness (HSEP) programs exist in diverse interdisciplinary settings (Comiskey, 2014; Simons-Rudolph, 2020). The subject matter of their curricula is multi-faceted and far less homogenous than traditional academic disciplines such as political science and sociology, with interests and skill sets encompassing various technical, historical, and policy frameworks. Within this instructional landscape, some topics challenge accessibility—making content approachable and its application comprehensible. Cybersecurity is one such topic. Whyte (2021) notes that developing cybersecurity, cyber conflict, and cybercrime curricula for social science students is inherently tricky. These students sometimes find it challenging to comprehend the relevance of technical points for policy, theory, and practice. Conversely, technically oriented students often find difficulty in setting operational details amid socio-strategic content. Ultimately, linking levels of analyses for cybersecurity as a critical dimension of homeland and national security studies is a formidable task for instructors.

This article adds to the body of knowledge on active and experiential learning in cybersecurity and the social sciences (Shaw, 2004; Asal, 2005; Knight & Wood, 2005; Asal et al., 2017). The article delineates student and faculty perceptions of a *hack-along*, a simulated cyber operation. The hack-along experience guides students through offensive and defensive cyber operations with expert voices akin to the oft-utilized staff ride model of hands-on learning (Becker & Burke, 2012; Nussbaum, 2016).

The article begins with an overview of the cybersecurity challenge for HSEP programming before introducing the hack-along as a distinct, novel, and versatile tool for engaging students of all backgrounds and enabling them to build a conceptual map that bridges the operational and strategic contexts of cyber operations. Then, the article describes the results of experiences employing the hack-along in the cybersecurity curricula of the nation's oldest HSEP program—at Virginia Commonwealth University (VCU)—and describes opportunities for adaptation and customization.

THE CYBERSECURITY CHALLENGE FOR HSEP PROGRAMS

The context for developing this experiential learning activity is the broader development of the cybersecurity curricula for undergraduate and graduate students at VCU within the HSEP program over the past five years. As has been the case for many homeland security and related programs in the past decade (Simons-Rudolph, 2020), the HSEP program at VCU—the first HSEP program in the nation—has adopted cybersecurity as the core of its program.

The focus on cybersecurity presents a range of challenges for instruction and pedagogy. Among the hundred undergraduate and several dozen graduate students in any given term, there are diverse backgrounds and interest areas in which learning about cyber issues might be relevant. Most students have limited technical knowledge but have some conventional liberal arts and public policy training. Many students have some experience with narrow cybersecurity issues, often as an area encountered in a public sector internship or employment circumstances (net neutrality, data record security, healthcare management). Some students leave the HSEP program to pursue cybersecurity-related employment. Many enter public or private service positions with significant cyber roles, such as public health data security and law enforcement. The challenge in teaching such a diverse student body is constructing curricula that cut across what is known about cybersecurity in social science programs, business schools, law schools, and engineering coursework to produce something distinctly HSEP. Such curricula need to be augmented with active and experiential learning to force non-technologists and policy-minded students to form a robust conceptual map of the issues.

In recent years, the HSEP program at VCU accomplished these goals with a complete overhaul of its course offerings related to cybersecurity. Compared to coverage of cyber topics in coursework focused on varied elements of the HSEP field—such as constitutional and legal issues, terrorism, or public health management—cybersecurity is now centralized mainly under core undergraduate and graduate course offerings. These courses aim to move HSEP students from broad information and technology security principles to narrower topics in cyber strategy, cybercrime, and various legal and policy issues. Now, courses on cybersecurity, cyber policy, and cyber warfare incorporate technical, historical, political, strategic, and legalistic perspectives into the interdisciplinary learning environment of the HSEP program. These are strengthened by experiential learning across several formats, including video games, tabletop exercises, student-driven branching scenarios, and a full range of classroom thought exercises. Few activities, however, are as effective at helping students build better conceptual maps of the overlapping issues they study as the hack-along.

THE HACK-ALONG AS A TOOL FOR BRIDGING LEVELS OF ANALYSIS

In considering how best to offer students experience in the operational realities of cybersecurity, it was necessary to bear in mind the context of HSEP education. Unlike in more conventional cybersecurity instruction, where the scope of the experience is relatively narrow to organizational infrastructure and interests, HSEP cyber practitioners, planners, and strategists must consider defensive and offensive issues across the gamut of national critical infrastructures, military-intelligence apparatuses, and more. Two apparent parallels for building such an experience were law enforcement ride-alongs (Payne et al., 2003) and the staff ride. Police ride-along activities are designed to let citizens observe the workings of their law enforcement services in different settings and have often been used for student training. Staff rides are historical walkthroughs of battlefields and other event sites that give students or professionals a more tangible feel for the progression of circumstances in a given episode than might otherwise be possible.

The hack-along combines the focus on observing cyber operators at work with historical or hypothetical learning that ties the stakes of digital operation to broader homeland and national security issues. Across three terms in 2021 and 2022, I ran two distinct versions of the hack-along that would be easily replicable by instructors at programs similar to that at VCU. First and most substantially, I paired with graduate students in engineering to develop several simulated hacking environments based on hypothetical and historical scenarios that students had the opportunity to discuss and learn about in conventional course settings. These simulated environments employed some custom visualizations alongside Kali Linux in much the way ethical hacking courses do to allow students to experience various tools in a robust, realistic network setting (Najera-Gutierrez & Ansari, 2018). The idea was that environments be set up as realistic and complex as possible so those subject matter experts could guide HSEP students through hacking scenarios from defensive and offensive perspectives.

Two scenarios were developed for use in the initial trial runs of the hack-along. The first was entirely hypothetical, an attempt to compromise the infrastructure systems of an electrical grid operator. Students were given basic information on a fictitious company (analogous to many real-world grid operators they had studied) and discussed the rationale for potential malicious attacks. Facilitators then “attacked” the company, walking students slowly through their thought processes, the decisions they made or could make, and the payoffs and probabilities involved in specific actions. In a second session, facilitators split up, with some guiding students through a defensive effort as another repeated the initial attack. The second scenario followed a similar operational approach to walking students through attack and defense approaches. Here, however, the environment was designed to simulate a historical incident that students were familiar with from case study analysis, in this case, a significant espionage operation conducted against U.S. government systems in the 2000s thought to be the work of Russian security services.

A second version of the hack-along, conducted in early 2022, took a slightly different approach to experiential learning by taking advantage of the ongoing conflict between the Russian Federation and Ukraine. Here, an external facilitator operating as a liaison between Western defense establishments and the volunteer “IT Army of Ukraine” introduced students to the many

tools, resources, and coordinating methods used to organize the actions of thousands of volunteer hackers against targets linked to the Russian government. This hack-along did not tie the classroom experience to hacking activities or non-public resources for legal and safety reasons. Nevertheless, the experience successfully provided another form of hands-on instruction on cyber operations to HSEP students.

ASSESSING THE APPROACH

Students were prompted to reflect on the hack-along activity along three lines. First, each activity was followed by a debriefing session with student participants, lasting no more than 90 minutes. These took place between instructors and students in a semi-structured focus group setting. Facilitation questions were geared toward helping students unpack their initial expectations, establish what they learned from the operational walkthroughs, and define new takeaways they gleaned from the experience. In particular, the discussion was geared toward linking the operational experience to the strategic circumstance of the hacks in each scenario. Feedback was highly positive, and many students claimed a breakthrough moment in thinking about how the operational realities of cyber defense and offense affect strategic planning in settings they were more familiar with (i.e., at high-level organizational decision-making). Second, students were also invited to enumerate these takeaways in a draft assessment paper they could submit for credit within a week of the debrief session. Students were explicitly assessed on their ability to link operational decision points with theoretical assumptions or policy articulations relevant to the cases. Finally, students were invited to include a section in their final class projects—which focused on describing advanced persistent threat (APT) actions to the fundamentals of a foreign state's foreign policymaking—that assessed the degree to which macro interests and policy environments might constrain or incentivize specific operational choices. The results were exciting, with many students demonstrating a firm grasp of how institutional culture, organizational preference, and the contours of international competition might contribute to different ways of cyber war among national or criminal entities.

Perhaps the most significant takeaway for me, as the instructor in developing and executing the prototype iterations of the hack-along, was the apparent need to embed the activity amid course content that had revealed the dots to students and would then be connected during the walkthrough. The HSEP graduate curricula at VCU entailed two activities in particular. First, students were introduced to concepts and threat types from day one of their coursework alongside extensive case examples. Initial weeks built an understanding of web architecture, cyber threat models, best information security practices, and U.S. experiences with cyberspace as a national security concern via exploration of cases such as Cuckoo's Egg, Moonlight Maze, Buckshot Yankee, Stuxnet, Operation Orchard, and more.[1] Second, students supplemented this content consumption with "in-class" playthroughs of a video game—specifically, the 2015 game Hacknet—that gradually introduced students to the tactical ideas and concepts behind cyber

[1] Information on all of these episodes, as well as the terminology employed (e.g. "APT") can be found in several sources, including Whyte and Mazanec (2018), Singer and Friedman (2014), and Van Puyvelde and Brantly (2019).

operations. Even where progress in the game was slow for many students, this activity built a general idea of what hackers do when they attempt to compromise a target system. Then, by mid-term, students were ready to experience the hack-along," which effectively ties learning about cybersecurity and cyber conflict at these distinct levels of analysis.

OPPORTUNITIES FOR UPGRADING AND CUSTOMIZATION

Students received this activity positively, with many citing it as an unusual opportunity to view the operational side of cybersecurity in the context of macro homeland security considerations beyond simple thought exercises or case readings. Given this, I believe the hack-along activity and concept are highly relevant for HSEP education. Moreover, the concept is highly portable in several settings. Some resource capacity is required to run such an experiential learning activity. However, as demonstrated with the initial run-throughs of the hack-along at VCU, this capacity can be built in partnerships with knowledgeable stakeholders inside the institution. Colleagues or graduate students in cybersecurity and engineering schools, business schools, or even within HSEP units at some institutions are excellent resources for standing up such activity, not least because of the pedagogical and research value often found in participation for those partners.

Over the next several years, our goal is to develop a catalog of scenario environment experiences that will allow HSEP students to learn about significant incidents in U.S. history with cybersecurity as a national security concern and relive the operational moments therein. There are opportunities for those interested in the hack-along method of instruction to tailor experiences to state and industry-specific circumstances. Moreover, the hack-along concept stands to help strategic planning courses and initiatives within HSEP programs with an ability to consider the impacts and threat severity of potential future events, adding a value proposition for these programs beyond just greater accessibility for students being increasingly asked to gain expertise in cybersecurity issues.

CONCLUSION

The homeland security-emergency management program at VCU will continue to explore the hack-along concept and develop yet further iterations of the activity to best synergize with the needs of employers and the evolving context of global cyber-conflict conditions. At full enrollment, we expect several dozen students to have experienced the hack-along by the end of AY 2024 and that the benefits of the activity will become even more fully realized in the contributions of the many students who graduate into various homeland security and emergency preparedness agencies.

REFERENCES

Asal, V. (2005). Playing games with international relations. *International Studies Perspectives*, *6*(3), 359-373.

Asal, V., Fahrenkopf, N., Jadoon, A., & Hwang, I. (2017). Prisoners at midnight: Introducing undergraduate students to the advantages and disadvantages of quantitative analysis through a simulation exercise. *European Political Science*, *17*, 621-633.

Comiskey, J. (2015). How do college homeland security curricula prepare students for the field? *Journal of Homeland Security Education*, *4*, 20-40.

Knight, J. K., & Wood, W. B. (2005). Teaching more by lecturing less. *Cell Biology Education*, *4*(4), 298-310.

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web penetration testing with kali linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Nussbaum, B. (2016). Leveraging the staff ride for active learning in public safety management. *Journal of Homeland Security Education*, *5*, 1.

Payne, B. K., Sumter, M., & Sun, I. (2003). Bringing the field into the criminal justice classroom: Field trips, ride-alongs, and guest speakers. *Journal of Criminal Justice Education*, *14*(2), 327-344.

Shaw, C. M. (2004). Using role-play scenarios in the IR classroom: An examination of exercises on peacekeeping operations and foreign policy decision making. *International Studies Perspectives*, *5*(1), 1-22.

Simons-Rudolph, J. M. (2020). *An examination of academic education for homeland security.*[Masters thesis, Naval Postgraduate School. Monterey, CA].

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford University Press.

Van Puyvelde, D., & Brantly, A. F. (2019). *Cybersecurity: politics, governance and conflict in cyberspace*. John Wiley & Sons.

Whyte, C., & Mazanec, B. (2018). *Understanding cyber warfare: Politics, policy and strategy*. Routledge.

Whyte, C. (2021). Using Mini-Games to Teach Cyber Issues to Social Science Students. *Journal of Political Science Education*, *17*(sup1), 215-225.