Utah State University

DigitalCommons@USU

Resilient Pedagogy   Empower Teaching Open Access Book Series

6-7-2021

Chapter 5- Lessons from Anticipatory Intelligence: Resilient Pedagogy in the Face of Future Disruptions

Briana D. Bowen
Utah State University, briana.bowen@usu.edu

Follow this and additional works at: https://digitalcommons.usu.edu/resiped

Part of the Higher Education Commons, Online and Distance Education Commons, and the Teacher Education and Professional Development Commons

UtahState University
MERRILL-CAZIER LIBRARY

5.

LESSONS FROM ANTICIPATORY INTELLIGENCE: RESILIENT PEDAGOGY IN THE FACE OF FUTURE DISRUPTIONS

Resilient Pedagogy in the Face of Future Disruptions

Briana D. Bowen

The COVID-19 pandemic has disrupted universities across the globe in unprecedented ways, requiring many teaching faculty to reexamine and transform approaches to pedagogy. As higher-education institutions have grappled with various methods of hybrid and remote delivery in an effort to best preserve student instruction through the pandemic, most have fervently looked ahead for a more satisfying "new normal." Yet this moment of unease and transformation is one of critical opportunity for universities and their teaching faculty. Educators are seeing in vivid form how an unexpected "threat"—in this case, a global health challenge—can profoundly disrupt pedagogy, and the immense adaptive innovation necessary to preserve universities' most important functions through a sustained period of difficulty. Equally important are lessons concerning the varying degrees of success experienced between institutions based on different levels of proactive planning and the quality of resilience-building strategies.

The reality is that a pandemic is far from the only major disruptive event that could impact teaching on a localized or global scale. In an increasingly complex and interconnected world facing growing disruptions from climate change and the rapid pace of technological advance, faculty are better served by looking at the COVID-19 pandemic as a template and a testing ground for future disruptions rather than a once-in-a-generation challenge. The diversity of these future disruptions and their impacts on university teaching may range from the short-term, acute, and localized (such as a cyberattack taking down university internet servers for a day) to the long-term, chronic, and large-scale (such as a severe solar weather event that could black-out portions of the US electric grid for weeks or months). There is real value, therefore, in looking ahead to the horizon of possible disruptions to pedagogy and examining how not just administrators but individual teaching faculty can play an active role in building more resilient university communities.

This chapter offers a practical tool kit for faculty to cultivate a mental orientation toward planning, adaption, and innovation in the face of future disruptions to university life. These insights are drawn from the field of anticipatory intelligence, which concentrates on emergent disruptive security challenges and their

implications for human society. An expert grasp on specific potential threats is not required in order to benefit from the thought exercises offered here, nor is it the goal of this chapter for faculty to gain perfect foresight of the next major disruption. Rather, engaging with these tools, including the 4R resilience modeling framework developed by Utah State University's Center for Anticipatory Intelligence (CAI), can offer faculty a foundational primer in anticipatory thinking and proactive planning to better prepare for the continuity of excellent teaching despite a range of challenges in uncertain times to come.

Understanding Anticipatory Intelligence

To equip faculty with a set of practical tools from the anticipatory intelligence domain, this chapter will provide a brief stage-setting primer on the field of anticipatory intelligence, present a simplified framework for assessing categories of potential disruptions to university teaching, and walk through the 4R resilience modeling framework with specific application to pedagogy.

The field of anticipatory intelligence is a developing area of interdisciplinary scholarship whose origins hail from the professional world of national security. The concept of anticipatory intelligence started to gain broad attention in the US intelligence community around the early 2010s as a result of the rising complexity and heterogeneity of challenges facing US national security interests after 9/11 (Kerbel, 2019, para. 2, 6). By the end of the decade, the US National Intelligence Strategy highlighted anticipatory intelligence as one of three key priority areas for US intelligence agencies (Office of the Director of National Intelligence [ODNI], 2019a, p. 7, 9). A cousin concept can also be found in Russian military doctrine—*predvideniye*, or "foresight"—and actually has a longer pedigree of active practice (Bartles, 2016, p. 31). Defined in the US National Intelligence Strategy:

> Anticipatory intelligence involves collecting and analyzing information to identify new, emerging trends, changing conditions, and undervalued developments, which challenge long-standing assumptions and encourage new perspectives, as well as identify new opportunities and warn of threats. . . . Anticipatory intelligence explores the potential for cascading events or activities to reinforce, amplify, or accelerate conflict. . . . [It] assesses risk, intelligence gaps, and uncertainties by evaluating the probability of occurrence and potential effects of a given development on U.S. national security. (ODNI, 2019a, p. 9)

In comparison to traditional strategic intelligence, which tracks data points and developments in known domains of US national security interest (e.g., the size, composition, and dispersion of the Russian nuclear weapons stockpile), anticipatory intelligence is oriented toward on- and over-the-horizon developments whose nature, implications, or intersection with other security challenges is unclear (e.g., could the rapid advance and democratization of gene-editing tools like CRISPR-Cas9 hold national biosecurity implications?).

As the field of anticipatory intelligence has grown in academia, it has been applied to a much broader scope of assessment than just US national security, ranging from global security down to organizational security and even to individual risk and security. In an increasingly complex world, these levels of security are becoming less distinct and discrete, and a rising range of threats hold implications for security on multiple levels simultaneously. For example, hurricanes slamming ashore with more ferocious strength due to longer incubation periods in a warming global climate not only displace communities through a region but can destroy crucial national defense assets (Achenbach et al., 2018). Advances in commercial drone technology have been an asset to photographers, but also to narcotrafficking cartels seeking novel ways to move product across national borders (Fiegel, 2017). Foreign national adversaries to the US government have used cyberattacks and cyberespionage against US private companies and universities to advance geopolitical goals (Brown & Singh, 2018; Asokan, 2020). To the extent that national security issues were once the exclusive jurisdiction of federal government agencies, a rising number are increasingly the concern of other public and private sector entities, including universities.

Utah State University's Center for Anticipatory Intelligence (CAI) has done much of the pioneering work in drawing over the concept of anticipatory intelligence from the national security space into the academic arena. Theoperational frameworks this chapter offers reflect CAI's approach to anticipatory intelligence and draw on the work of students in USU Anticipatory Intelligence academic programs. Because of this, a brief snapshot of CAI's structure and design may be useful to the reader.
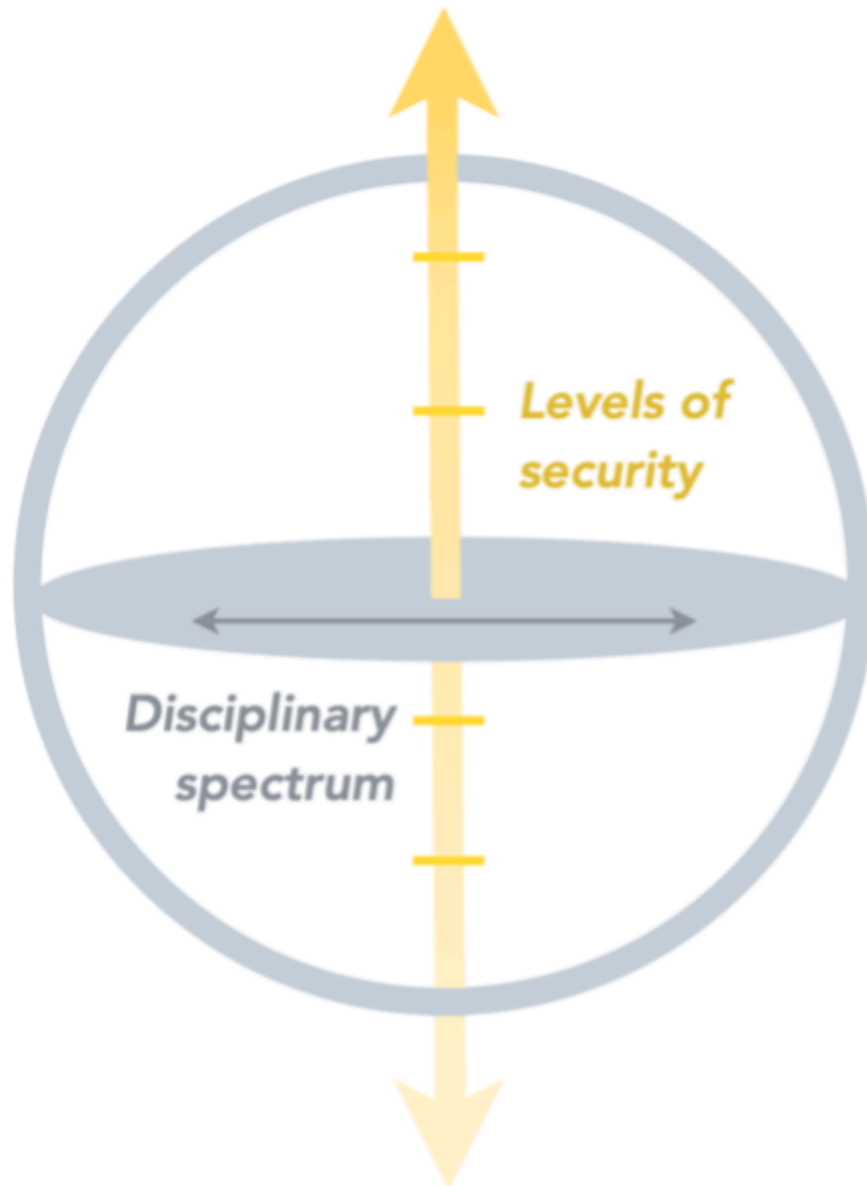
Figure 1 Scope of Focus for USU's Center for Anticipatory Intelligence

Responding to the complex intersectionality of emergent security issues, CAI's scope of focus encompasses levels of security from the international down to the individual domains and examines problem sets originating from or impacting the full disciplinary spectrum, incorporating STEM fields, the social sciences, and the humanities. These security challenges include intentional, malicious, and actor-driven threats; unintended consequences of human action or technology development; or environmental disruptors from anthropogenic or natural origins (CAI, 2020a).

Administratively located within USU's College of Humanities and Social Sciences, CAI is a fully interdisciplinary center with faculty collaborators and students at the undergraduate, master's, and PhD levels

collectively hailing from all eight USU colleges. CAI places a rigorously interdisciplinary orientation to security thinking and resilience design as its most central principle. This approach to anticipatory intelligence is prioritized because the vast majority of problem sets in this field fit under the categorization of "wicked problems"—deeply complex and interconnected issues with myriad stakeholders that are not fully preventable or solvable (Rittel & Webber, 1973)—and require a richly heterogeneous approach to make meaningful advances in threat mitigation and resilience building.

Threat and Resilience Frameworks

A principal goal for practical scholars and practitioners of anticipatory intelligence is to glean proactive insights into challenges that may be on or just over the horizon for an organization or industry—with a better-than-educated-guess sense of the disruptive intersectional dynamics that may come into play—thereby giving more lead time for institutions and individuals to prepare for the challenge and to head it off when possible or better absorb it when not.

Anticipatory intelligence thus has an intrinsic relationship to security thinking, emergency planning, and risk management, or the preparation and processes that go into designing secure systems and safe events. Naturally, these areas are by no means limited to the field of anticipatory intelligence, and most universities and large companies have established offices dedicated to this type of planning and assessment. In many institutions, however, these assessments are limited to specific *events* (e.g., a high-profile visiting speaker) or are focused on protecting against a specific *threat category* (e.g., cybersecurity) rather than surveying the frontier of both known and on-the-horizon challenges that could threaten or disrupt the system.

While a discussion of best practices for risk management and security offices is outside the scope of this chapter, this is a domain in which an anticipatory intelligence mindset could bring value to the proactive planning of universities and other institutions in order to have better informed and more productively imaginative institutional responses teed up for times of crisis. Building on this concept, the following sections offer a simplified tool kit that faculty can work through as a personal mental exercise or a group discussion with colleagues to envision general types of disruption to universities and develop responses for resilient pedagogy through a disruptive event or period. Teaching faculty as well as department heads and graduate program directors may be unaccustomed to viewing this type of assessment and planning as a personal or departmental responsibility, but engaging in these thought exercises can yield significant return on investment for individuals and institutions.

Simplified Threat-Assessment Framework

Because this chapter is concerned with a *specific impact* (disruption to pedagogy) to a *defined system* (higher education), isolating categories of disruptive *impacts* to teaching—rather than a comprehensive lineup of all possible sources of disruption—can serve as a suitable foundation for building features of resilience. This is because, first, the same "package" of adverse impacts to university instruction can originate from a wide range of disruptive sources, and second, in happy reverse, it is well established in evidence that a system designed to be robustly resilient against one threat is often significantly more resilient against a host of other threats, whether they are directly or loosely related. Therefore, faculty do not need to utilize a comprehensive threat assessment framework nor become experts in identifying the legion emergent challenges across the "threatscape." Instead, this simplified framework can be used to think through a basic matrix of disruptive impacts affecting university pedagogy:
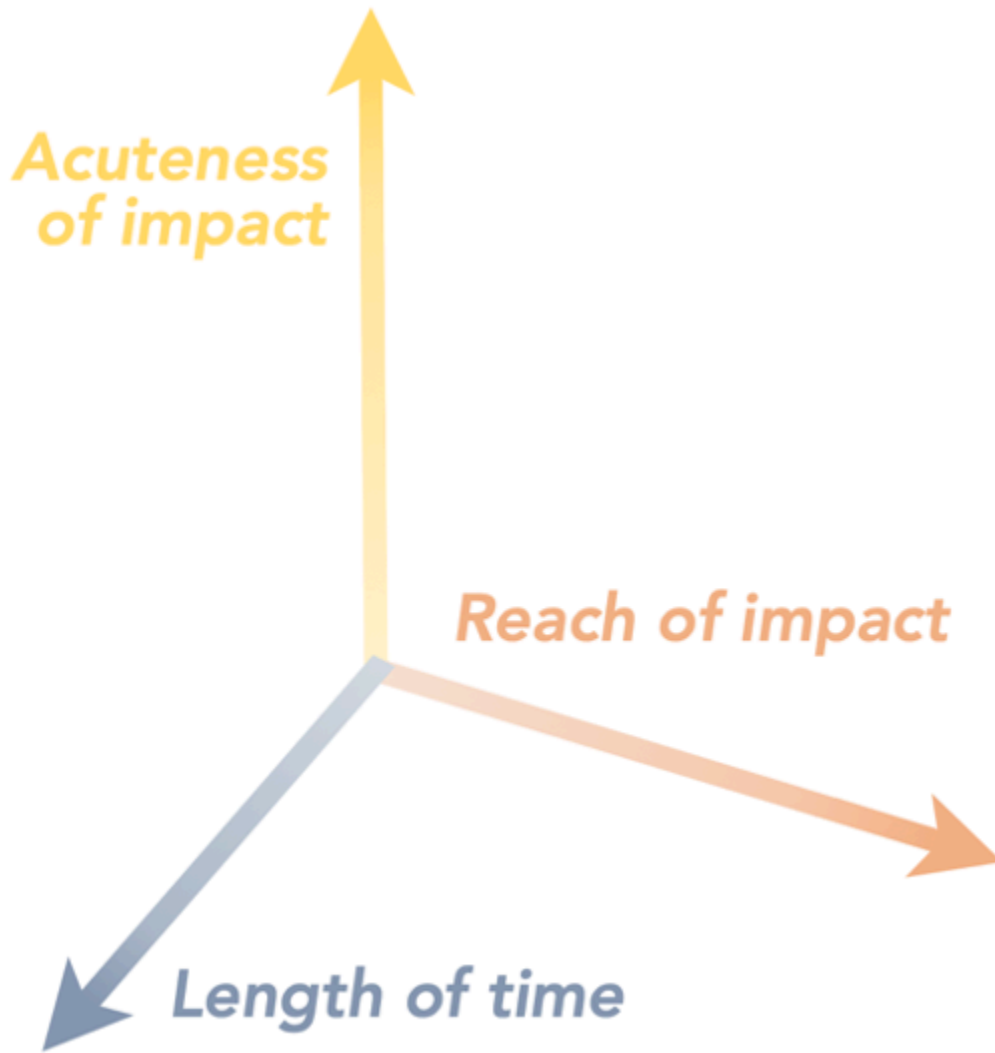
Figure 2 Simplified Threat Model

Categories of Disruption to Pedagogy			
Reach of impact	Localized (individual/ department)	Campus-wide	Community-wide or beyond
Acuteness of impact	Inconvenience for teaching	Requires major adaptations in teaching	Makes teaching impossible
Length of time	Day or days	Weeks	Semester or longer

Figure 3 Simplified Threat Matrix

To illustrate a basic sampling of scenarios satisfying combinations of these categories, the following three examples assess how multiple types of threats could land teaching faculty in the same broad circumstances.

Reach of impact	Acuteness of impact	Length of time
Localized (individual/department)	Inconvenience for teaching	Weeks

Example 1

A disruption creating a *localized*, *weeks-long inconvenience for teaching* could originate from a sophisticated ransomware attack aimed at a university or personal computer on which a faculty member stores local files of lecture notes, past quizzes and exams, and class plans—encrypting all files and risking permanent loss if the demanded sum is untenable to pay or if the files are permanently corrupted even upon payment of the ransom. Likewise, a standard physical security breach could naturally land an individual in the same position through theft, damage, or mechanical failure of a computer whose files are stored locally, or through loss of single-copy printed teaching materials. In conditions like these, faculty are faced with weathering significant (and likely preventable) personal inconvenience as they continue usual instruction.

Reach of impact	Acuteness of impact	Length of time
Campus-wide	Makes teaching impossible	Day

Example 2

A disruption creating a *campus-wide, day(s)-long interruption to teaching* could originate from a severe cyberattack aimed at university servers that cuts off internet or user access to key online teaching platforms, making most instruction (especially in the remote teaching era) impossible for a day or several days while IT personnel work to restore internet access. Other campus-wide emergencies like region-specific extreme weather events (e.g., blizzard, tornado, hurricane) could have a similar impact. In cases such as these, teaching is simply made impossible for a short period and faculty are limited to cancelling classes and deciding how to best reschedule or revise coursework around the disruption.

Reach of impact	Acuteness of impact	Length of time
Community-wide or beyond	Major adaptations in teaching	Semester or beyond

Example 3

A disruption creating *community-wide, long-lasting effects requiring major adaptions* in teaching includes, of course, the situation that most universities around the world faced in 2020 due to the COVID-19 pandemic. But a severe solar weather event that unleashes large-scale disturbances on the ground-based electric grids and space-based assets that underpin much of modern life (including power, internet, GPS, and more) could also land universities in the same type of long-term, major-adaptation response zone—as could a sizeable earthquake that compromises physical infrastructure, food and water supply, and basic services for the broader community or region. In cases like these, faculty must negotiate two phases: the "moment of impact" disruption that may interrupt teaching for a period while the university or broader community recuperates to a new functional baseline, and the sustained disruption period, during which an adapted "new normal" is implemented for university instruction.

Visualizing Personalized Scenarios

Using these brief snapshots as a kickstart, faculty can gain the most value by employing the simplified threat assessment framework to think through permutations of the matrix above and visualize a range of plausible scenarios that could yield such impacts for their own institutions. Assembling this personalized list of scenarios best prepares faculty to directly and productively apply the 4R resilience modeling framework below. The thought exercise of compiling this list can be conducted individually in a quiet brainstorming

session, a collaborative tabletop exercise in department or college meetings, an interdisciplinary workshop with campus colleagues, or a class exercise with students interested in the concept of resilience. Department heads, graduate program directors, and other faculty with administrative responsibilities related to teaching may find particular benefit in doing this exercise with key stakeholders. As noted above, the intent of this simplified framework is not to perfectly predict or foresee specific events, but rather to usefully draw on productive imagination to glean more sophisticated insights into the intersecting challenges, complicating variables, and human dynamics that could significantly shape a disruption down the road. Conducting thoughtful "mental imaging" of a diverse array of scenarios cultivates a mental orientation toward planning, adaption, and innovation and equips faculty to design resilience plans for pedagogy that are tailored to their individual circumstances. Mental imaging also offers an opportunity to bolster personal resilience—conceptually "practicing" a variety of disruption scenarios actively lessens shock and stress when a disaster does strike, and it heightens nimbleness and confidence in prepared reactions and adaptions.

For those interested in seeking a better sense of potential disruption sources, a robust stockpile can be found in the annual *Worldwide Threat Assessment* produced by the Office of the Director of National Intelligence (2019b) and the *Homeland Threat Assessment* generated by the US Department of Homeland Security (2020). In addition, USU's Center for Anticipatory Intelligence produces the *CAI Student Research Reports* (2020b) white paper series, offering an open-source reservoir of research specifically oriented toward tracking the spectrum of emergent security challenges.

4R Resilience Modeling Framework

Armed with a sense of the possible categories of disruption to university teaching, faculty are equipped to engage next with the 4R *resilience* modeling framework. Within the field of anticipatory intelligence, the term resilience is conceptualized as the ability of a system to rebound quickly from disruption and maintain its most essential integrity and functions through periods of friction or stress. Drawing on a wide interdisciplinary survey of literature, including work spearheaded by USU Anticipatory Intelligence students (Johnson, et al., 2019), CAI's 4R resilience modeling framework captures a range of best practices for building systemic resilience around four elements: *resistance*, *recovery*, *retention*, and *resurgence*. These components are not intended to be necessarily linear or chronological and sometimes naturally overlap in areas.

The 4R framework offered below has been adapted to specifically assess how university faculty members might build resilience into their own practice of pedagogy through a range of disruptive events. This framework is designed to "click in" to the simplified threat assessment and personalized scenarios developed above and can be mentally worked through in the same types of individual or collective settings previously suggested.

Resistance

What can be done to mitigate or prevent the disruption from happening?

The Concept

Resistance planning centers around measures that can be taken to interdict a threat before it hits the system. In any setting, decisions made by stakeholders to achieve positive resistance are rife with one of the fundamental premises of security thinking: security is always a question of *trade-offs* with other values or goods—convenience, personal freedom, accessibility, and so forth (Schneier, 2003). For the challenges across the threatscape that are possible to proactively mitigate or prevent at a reasonable trade-off level, planning and investing in resistance measures is often the sensible move from a rational economic lens: An ounce of prevention does, in fact, shake out to about a pound of cure. Furthermore, in an increasingly complex and hyper-connected world, resistance measures that are taken—or fail to be taken—by an individual against a specific threat can ramify throughout the security and resilience of an entire system.

Resistance in Action

In a university setting, some resistance-building decisions simply fall outside the jurisdiction of typical faculty members, residing primarily with administrators and facilities personnel. But as discussed below, these resistance measures have important effects on individual faculty, and sometimes the line of shared responsibility for shoring up resistance lies closer to faculty than expected. A useful illustration of resistance measures in action is the physical security of university facilities. For university buildings with sensitive contents or operations, emphasis on conscious facility design and location, deterrents like perimeter or building surveillance, and multiple-redundancy access requirements (e.g., passcode, dual authentication, and biometric scan) can significantly enhance security. Yet from the era of medieval fortresses down to modern secure research or teaching laboratories, total impregnability is a fantasy—any system ultimately has weaknesses if the scale or willful determination of the threat is significant enough or even if human error has one of its more spectacular days. The goal of resistance instead becomes using finite resources to make a security breach simply *hard enough* that most willful actors or natural disasters will have little meaningful effect in disrupting the core functions of the system.

With each layer of resistance measures installed, however, trade-offs in the form of accessibility accumulate. Some years ago, the author participated in organizing a conference of academics and policy experts collaborating on a federally funded grant project. Even though the conference and project were to be fully conducted at the unclassified level, the conference was held at a secure facility affiliated with one of the

project's principal investigators. In order to enter the building, attendees had to relinquish phones, laptops, thumb drives, and other electronic devices for the day's full eight-hour session—an oddity, mildly put, in the modern world. While the enhanced physical security of the space guaranteed the uninterrupted privacy and focus of the proceedings, the convenience tax on attendees was steep. When considering the potential threats or disruptions averted by physical resistance measures in a university setting (intellectual property theft; vandalism; manipulation of records; physical harm to faculty, staff, or students), there is little question of the value at stake, but the security trade-off threshold that administrators and faculty agree on will be calibrated differently between a standard office suite and an advanced virology lab.

Application to Pedagogy

In some domains, faculty may have significant capacity to personally implement meaningful resistance measures against possible disruptions to pedagogy. One area where individual resistance can combat a pervasive threat is faculty cyber hygiene. While some progress has been made in recent years by institution-wide mandates to implement dual authentication and require regular password changes, personal cyber hygiene among many faculty remains less than auspicious. Careless habits like using an institutional single-sign-on (SSO) password for other accounts, failing to use a virtual private network (VPN), letting vigilance against spear phishing slide, or neglecting home router and smart device cybersecurity can allow malicious actors to seize university credentials and penetrate systems to do mischief that may have far-reaching impacts. The disruptions to pedagogy that can derive from the universe of cyberattacks are myriad—from the individual inconvenience of the ransomware scenario described above to a more serious and damaging attack on university-wide services or infrastructure. The additional rising risk of intellectual property cybertheft should drive home to faculty members both the personal and institutional importance of wearing the digital facemask of good cyber hygiene. Though not a hermetic seal between the individual and the dangerous elements of the cyber environment, a serious and committed regime of personal resistance measures in cybersecurity is a sensible trade-off in helping to contain the spread of harmful elements that could have much wider negative systemic impacts if unchecked.

Self-Assessment Questions

With a personalized list of possible disruption scenarios in hand, faculty can engage in resistance planning by conducting a mental "mapping" exercise with these questions:

- For threats or disruptive challenges that could directly impact me or my department, what measures are within my power to actively decrease or prevent the likelihood of a disruption to my teaching? How can I sustainably implement these measures?

- Are there any specific security issues that could originate in or penetrate through my department and impact teaching in the wider university community? Have I put appropriate measures in place to

mitigate or prevent these?

- What are the right balances for me or my department in elevating resistance against certain types of threats or challenges given the actual cost and opportunity cost of the associated trade-offs?

Recovery

What can be done to rebound from disruption to a minimum functioning threshold?

The Concept

Recovery shifts gears to assess the best responses once a disruption to a system has taken place, perhaps despite best efforts to prevent it. In general terms, the goal of the recovery phase is to move a system out of a state of acute disruption, in which the system's core functions have been halted, to one of at least baseline operations. The nature and length of recovery hangs on the scope and severity of the disruption itself: The recovery phase may be limited to reaching the minimum functioning threshold for the system and learning to make do with a "new normal" (this leads into *retention*, below), or it may offer a path all the way to a complete rebound from disruption. In either case, recovery measures are about the crucial zero-to-sixty acceleration to most efficiently get key system elements back up and running after a disruption.

Recovery in Action

A perennial worry among threatscape watchers is the unlikely but grim possibility of a significant solar weather event resulting from a coronal mass ejection (CME) or a solar flare hitting the Earth, impacting both critical ground- and space-based assets with electromagnetic radiation, magnetic field-embedded plasma, and energetic charged particles. Depending on the strength of the solar weather event, radiation and energetic particles could short out in-orbit satellite constellations and magnetic field-embedded plasma could induce currents that surge through electric grids, blowing difficult-to-replace transformers and blacking out portions of the globe unlucky enough to take the direct brunt of the radioactive debris (Fraley, 2020, pp. 4–7). In both the mild (days to weeks of recovery) and apocalyptic versions (18+ months of recovery) of this scenario, one central point is vividly captured: electricity and the internet are the two "single points of failure" in modern life, upon which nearly all other systems of contemporary human society rely. Blackouts can originate, of course, from a wide range of natural or willful sources—similar impacts for more limited geographic areas could derive from malicious actors carrying out a physical attack or cyberattack on critical infrastructure like transformers or internet exchange points, or simply from a major storm that takes down a significant number of power transmission lines in a region.

We do not have a version of modern university life that operates without electricity and internet, meaning that resilience in this genre of disruption centers around recovering to basic operational levels of power and internet connectivity. As with most wide-scale challenges, external entities would play a crucial role in the mechanics of recovery from any blackout, tending to damaged portions of the electric grid and restoring service in stages to communities. The more severe a disruption of any kind, the greater the number of recovery elements that must be handled primarily at government or university leadership levels—and, obviously, there are some catastrophic challenges during which regular university functions simply would not be the priority for a stretch. But even in these rarer cases, as well as more modest and probable disruptions, individual faculty would still be responsible for a host of important recovery measures, beginning with emergency communications to and from students, modifying classes and coursework around the blackout period (literal or metaphorical), and figuring out how to rebound to a new minimum functioning threshold within their own pedagogy as soon as university conditions allow teaching to resume. As the COVID-19 world shifts ever more rapidly into the virtual universe, no institution should fail to have a weather eye on these two single points of failure and be actively considering the zero-to-sixty recovery plans within the institution's power to rebound to a baseline level of core functions—even if an acceleration to previous freeway cruising speeds is not possible for some time.

Application to Pedagogy

When the COVID-19 pandemic hit critical scale in March 2020, most university faculty across the United States experienced some version of the transition that Utah State University implemented in shifting all Spring 2020 classes to fully remote instruction. Over the course of four days, faculty needed to quickly assess how to reconstruct courses in order to go from a state of totally suspended instruction to a new minimum functioning threshold in order to finish out the semester. Despite the steep and turbulent learning curve this placed on faculty, the COVID-19 transition at USU and many other universities is a prime example of quick recovery to a new operational normal that allowed instruction to then continue through a period of heavy societal disruption. While federal, state, local, and university leadership each had crucial decision-making roles in the policy responses to the pandemic in that interval, very few faculty members escaped the rigorous task of designing their own recovery plans essentially overnight. Assessing individual-level recovery strategies for rebounding pedagogy from *full-stop* to *basically workable* across a range of disruptions from the simplified threat framework can help orient faculty to the best practices necessary to more capably weather future recovery periods—small or great.

Self-Assessment Questions

Drawing on personalized scenarios for their own setting and institution, faculty can engage in proactive recovery planning by considering these questions:

- What are the key ingredients I need in order to hit baseline functionality in my teaching? How could I develop a pedagogical "72-hour kit" of sorts that could prepare me to quickly go from "zero to sixty" in a recovery scenario?

- What are localized "single points of failure" in my teaching—what disruptions would make it very difficult or impossible for me to continue to teach? Are there ways I could build backup or alternative mechanisms into these areas?

- Do I understand and have good communications with the stakeholders across my university who will be involved in recovery processes from stress or friction events? Have I considered backup communication methods with my students?

Retention

> What can be done in the midst of friction/stress to maintain core critical functions?

The Concept

Retention concentrates on retaining the most valued and important features and functions of a system through the duration of exposure to stress, friction, or disruption. Entering the retention phase implies that the system has reached at least a baseline level of functioning (recovery) if it has encountered a sharp disruption, but the system is compromised in its ability to operate at normal levels. Central to the planning and successful implementation of the retention phase is a deliberate assessment of what those most vital identities and operations of a system are, both tangible and intangible. This assessment is most useful when it includes not only the formal functions of a system (e.g., company sales, university instruction) but the value-based priorities and stylistic preferences that ideally define the system (e.g., company culture, certain classroom dynamics). Retention of these *core critical functions* through disruption or stress is dependent on the resilience of both the people and the material systems involved in sustaining these elements.

Retention in Action

Some years ago, the author attended a military training exercise in which service members were simulating a deployment to a foreign area of operations. The multiple-day exercise in full gear took place in a setting that approximated the basic conditions and tasks service members would be likely to encounter in a real deployment. Halfway through the exercise, however, a brilliant twist in the simulation was imposed: as a result of an imagined electronic warfare (EW) attack, service members "lost" the ability to use most electronic

devices and services, including standard communications and myriad systems that underpin military situational awareness and physical security. This development plunged service members into a brief *recovery* moment, figuring out how to scramble back to a minimum operating threshold, followed by a prolonged *retention* phase. With no option to simply stop or call it a day, service members had to determine how to sustain their primary mission—their core critical function as a military force—under significantly disadvantaged conditions. Participants moved quickly to develop new sustainable communication methods, implement amended logistics protocols, and make the best of low-tech physical security measures as the simulation stretched into subsequent days.

When facing challenges that fall in the middle-term to long-term categories of the simplified threat matrix, university faculty can expect a significant effort toward a retention mindset: assessing how to preserve one of their core critical functions—offering the highest realistic standard of excellence in teaching—through long-haul disruptions to university life. In a scenario of sustained local or national civil unrest that impacts university campuses, a faculty member's well-considered plan for sustainably retaining the most important substantive and stylistic elements of their teaching through the period of disruption would be a significant asset. When facing more localized disruptions, recovery and retention mindsets may sometimes naturally link together. For example, despite commitment to good cyber hygiene, a sufficiently sophisticated ransomware attack may still penetrate through an unfortunate faculty member's defenses, encrypting all local files and positioning the attacker to demand a hefty sum for their return or threaten their permanent loss. In this circumstance, the key to both recovery and retention lies with the proactive measures that have been put in place to ensure that such an attack will not cripple a faculty member's basic ability to continue duties including teaching, research, mentorship, thesis or dissertation supervision, tenure processes, grant management, and so forth. These measures often fall into the domain of *positive redundancy*, or alternate methods of guaranteeing a specific capability. For example, primarily storing files in a cloud server (especially a university-authorized one) and keeping a regularly updated offline encrypted external hard drive in a secure location both offer relatively low-cost ways for faculty to be able to circumvent the disruption of a ransomware attack and regain access to important or irreplaceable materials.

Application to Pedagogy

For threats that may impose lasting stress and disruption on university teaching, implementing a retention focus means identifying not only how to safeguard the basic mechanics of instruction but the value-based or stylistic features of teaching that are most important to a faculty member, program, or department. An illustration from my own experience was the task of determining how to preserve the most valued stylistic features of the USU Anticipatory Intelligence program through the disruptions imposed by the COVID-19 pandemic during 2020. The central organizing principle of the USU Anticipatory Intelligence curriculum is the concept of a richly interdisciplinary cohort of students that learns to function together as an analytic team, actively valuing the personal and disciplinary diversity that each cohort member brings—and the blind

spots they flag—for their fellow students as they collectively tackle "wicked problems." In a typical year, cultivating this culture involves dedicating a significant portion of class time in foundational courses to in-person exercises, intensive role-playing simulations, and in-state and out-of-state field trips that cumulatively develop a sense of problem-solving cohesion and interdependence between students that range from undergraduates in anthropology to master's students in data analytics and doctoral students in aerospace engineering.

In order to safeguard retention of this valued dynamic in the incoming 2020/21 cohort, the USU Anticipatory Intelligence program implemented innovations to accomplish these key "intangible" goals. Over the summer of 2020, several CAI faculty members and nearly a dozen CAI alumni from previous cohorts facilitated a virtual "boot camp" series for students in the incoming cohort, combining brief introductory lectures on curriculum concepts with breakout exercises that paired three or four incoming students with a CAI alum to work through a problem set and to be introduced to the principle of drawing on other students' divergent expertise and perspectives in problem solving. By participating in five virtual "boot camp" sessions over the summer, the 2020/21 cohort entered classes in fall 2020 already equipped with the central orientation of the program, which significantly enhanced interconnectedness and cohort cohesion despite the physical separation between in-person and remote students and the restrictions of social distancing. Through the fall 2020 semester, additional efforts to retain the program's organizing principles were built into hybrid class discussions, simulation exercises designed to accommodate both in-person and remote students, and a virtual adaptation of the annual CAI Speaker Series. Even in semesters with unfavorable teaching circumstances, consciously assessing and identifying the substantive and stylistic priorities of a course, department, or program can help inspire adaptations to better preserve the most valued core features during periods of chronic stress to a university system.

Self-Assessment Questions

As faculty consider the retention-planning questions below, another tool that may be useful to integrate is proactively simulating a friction or stress event in a tabletop exercise. Similar to the military training exercise described above, tabletop exercises allow a group of colleagues to envision and informally act out a specific disruptive scenario and can offer university faculty and administrators valuable insights into otherwise unforeseen stress areas, colliding challenges, and gaps in response plans. There is a robust body of resources from the government and policy realms on designing and running tabletop exercises to be both realistic and "intellectually liberating" (Ready.gov, 2020; UK Ministry of Defence [MOD], 2017; RAND Corporation, 2020).

- What are the most important substantive and stylistic elements of my teaching or programs I administer that I want to find a way to preserve even when experiencing disruption?

- What proactive measures could I begin trialing or instituting now that would better equip me to preserve these elements when facing localized or widespread disruption to normal teaching?

- What material systems do I rely on in my teaching? How could I proactively prepare to preserve my substantive and stylistic priorities during a period when these material systems are compromised or fail to function for a stretch?

Resurgence

> What can be done to leverage the opportunity of disruption to build a stronger system?

The Concept

Resurgence seeks to identify the windows of opportunity created when disruption impacts a system, forcing a reevaluation of system features that deserve to be recovered and retained—and those that perhaps should be jettisoned and replaced (Taleb, 2016). The resurgence orientation recognizes that both positive and negative elements of a system can be doggedly enduring, and sometimes moments of disruption or even crisis are a valuable catalyst to break down counterproductive features. A resurgence mindset views the overarching concept of resilience not as a mandate to preserve the system status quo in its entirety, but––drawing on the concept of retention above—as an opportunity to refine and actively expand the most positive features of a system in the wake of disruption.

Resurgence in Action

One of the most vivid recent examples of resurgence in the international security domain originates from the small Baltic country of Estonia, a former Soviet state bordering Russia. In 2007, Estonia was the target of a massive, multifaceted cyberattack campaign from Russia—one of the earliest such cyberattacks on record. The slew of digital assaults from various Russian actors on Estonian financial institutions, government services, and communications created mass confusion and disruption of some essential services while the Estonian government and private industries worked to sort out what was happening and restore services (Davis, 2007). This event left a searing impression in the Estonian national psyche, compounding existing anxieties about the potential threat Russia poses to Estonia's internal security and even its modern existence as an independent nation. In the wake of the 2007 cyberattacks, the Estonian public and private sectors united to implement a significant overhaul of its national approach to cybersecurity intended to make a repeat of the attacks impossible, bolstering Estonia's secure electronic identity system for citizens and creating the world's first "data embassies" in other nations that serve as offsite cloud backups for government data and

critical services (Ross, 2020; Organisation for Economic Co-operation and Development [OECD], 2018). Major efforts were also invested in training the Estonian population on individual responsibilities in cybersecurity as a matter of both personal resilience and national security (Ruiz, 2020, para. 4–6). When confronted with later cyber challenges—the WannaCry ransomware attacks, NotPetya malware attacks, and myriad issues presented by the COVID-19 pandemic—Estonia's resurgent cyber infrastructure allowed the country to weather the disruptions far better than many other nations (McLaughlin, 2019; "Covid-19 Strengthens," 2020, para. 3, 6). Estonia's experience underscores the broadly transferrable principle that building a system to be resilient against one category of threats significantly strengthens its ability to successfully weather a host of other challenges.

Application to Pedagogy

A range of resurgent transformations to academia can be envisioned on the other side of the COVID-19 pandemic, which has challenged many basic assumptions about the character of university pedagogy. Naturally, not every challenged assumption should result in a policy change, but the pandemic does provide an opportunity for a remarkably global conversation about a renewed and improved generation of best practices going forward. One concept that seems to hold significant promise as a resurgent innovation in academia is the integration of an online/remote participation option for public events like featured guest speakers, panel discussions, and student forums. Integrating a hybrid (virtual) participation option for events that are held primarily in-person creates a more open and inclusive global learning and information-sharing environment. Students and scholars across higher-education institutions have more rich opportunities to cross-pollinate research and findings, especially from universities that have specialized centers uncommon across most institutions (the University of Oxford's Future of Humanity Institute is a prime example). Students with disabilities or chronic health issues have better routes to more fully participate in university programs from afar when hybrid participation options are facilitated. Last, but not least, growing hybrid coverage of university talks and events gives evidence-based expert opinion a more frequent and public platform to be heard and shared in an era when disinformation prevails on the internet and facticity is undervalued. While I believe that the in-person elements of higher education are being shown to be more important than ever in the era of COVID-19, there is ample room to integrate a wave of high-value resurgent innovations deriving from the pandemic into university norms going forward.

Self-Assessment Questions

In creating space for resurgent adaptations in individual teaching portfolios, faculty may benefit from considering the following questions:

- In looking at disruption as an opportunity for resurgence, what elements of my teaching could merit reevaluation and restructuring during current or future disruptions I experience?

- As I adapt to disrupted teaching environments, what previously untouched skill sets, approaches, or platforms could I consider integrating into my pedagogy?

- Are there bureaucratic or cultural ruts associated with pedagogy that I, my department, or my university could positively interrupt as a result of stress or friction our system experiences?

Conclusion

A strikingly consistent lesson of history is that humans struggle to take seriously threats or challenges that they have not personally experienced. The opportunities for proactive resilience and innovation lost because of this are myriad—and unnecessary. By mentally engaging with a range of productively imaginative disruption scenarios and considering individually tailored resilience strategies to address them, university faculty can equip themselves with greater personal confidence in their own ability to weather future disruptions. Furthermore, faculty can develop enthusiasm for renewed and improved adaptions in teaching that are inspired by active resilience building. Full university communities—faculty, administrators, staff, and students—benefit when anticipatory thinking is applied to cultivate a rich communal and collaborative orientation toward resilience through planning, adaption, and innovation.

References

Achenbach, J., Begos, K., & Lamothe, D. (2018, October 23). Hurricane Michael: Tyndall Air Force Base was in the eye of the storm, and almost every structure was damaged. *Washington Post*. https://www.washingtonpost.com/national/hurricane-michael-tyndall-air-force-base-was-in-the-eye-of-the-storm-and-almost-every-structure-was-damaged/2018/10/23/26eca0b0-d6cb-11e8-aeb7-ddcad4a0a54e_story.html

Asokan, A. (2020, October 15). *Iranian hacking group again targets universities*. Data Breach Today. https://bit.ly/3mxWQDs

Bartles, C. K. (2016). Getting Gerasimov right. *Military Review*, *96*(1), 30–38. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art001.pdf

Brown, M., & Singh, P. (2018, January). *China's technology transfer strategy* (Rep.). Defense Innovation Unit Experimental [DIUx]. http://nationalsecurity.gmu.edu/wp-content/uploads/2020/02/DIUX-China-Tech-Transfer-Study-Selected-Readings.pdf

Center for Anticipatory Intelligence [CAI]. (2020a). *Mission*. https://www.usu.edu/cai/about/mission

Center for Anticipatory Intelligence [CAI]. (2020b). *Student research*. https://www.usu.edu/cai/student-research/index

Covid-19 strengthens the case for digital ID cards. (2020, September 05). *The Economist*. https://www.economist.com/leaders/2020/09/05/covid-19-strengthens-the-case-for-digital-id-cards

Davis, J. (2007, August 21). Hackers take down the most wired country in Europe. *Wired Magazine*. https://www.wired.com/2007/08/ff-estonia/

Fiegel, B. (2017, July 5). Narco-drones: a new way to transport drugs. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/narco-drones-a-new-way-to-transport-drugs

Fraley, E. (2020, April). *US security threatened by solar storm impacts on earth- and space-based technologies*. CAI Student Research Reports. https://www.usu.edu/cai/student-research/studentpaper-fraley

Johnson, J., Bodine, T., Brazell, J., Cragun, H., Cragun, L. Crookston, B., Funk, R., Gillespie, M., Hansen, D., Hugh, B., Miner, C., Penner, H., Porter, S., Schafer, D., Sproul, S., Turner, E., Vance, J., Warren, E., & Wilkinson, C. (2019, April). *Resilience framework* [Unpublished paper]. Center for Anticipatory Intelligence, Utah State University.

Kerbel, J. (2019, August 13). *Coming to terms with anticipatory intelligence*. War on the Rocks. https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/

McLaughlin, J. (2019, July 2). *How Europe's smallest nations are battling Russia's cyberattacks*. Heinrich Böll Stiftung: Washington, DC Office. https://us.boell.org/index.php/en/2019/07/02/how-europes-smallest-nations-are-battling-russias-cyberattacks

Office of the Director of National Intelligence [ODNI]. (2019a). *National intelligence strategy of the United States of America* (Rep.). https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019

Office of the Director of National Intelligence [ODNI]. (2019b). *Worldwide threat assessment of the US Intelligence Community* (Rep.). https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—SSCI.pdf

Organisation for Economic Co-operation and Development [OECD]. (2018). *Case study: The world's first data embassy – Estonia*. OECD Embracing Innovation in Government: Global Trends 2018, 42–44. https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf

RAND Corporation. (2020). *Wargaming*. https://www.rand.org/topics/wargaming.html

Ready.gov. (2020). *Exercises*. https://www.ready.gov/business/testing/exercises

Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169. https://link.springer.com/article/10.1007/BF01405730

Ross, M. (2020, April 03). *Finding your identity: Solving the digital ID verification challenge*. Global Government Forum. https://www.globalgovernmentforum.com/finding-your-identity-solving-the-digital-id-verification-challenge/

Ruiz, M. (2020, February 14). To bolster cybersecurity, the US should look to Estonia. *Wired Magazine*. https://www.wired.com/story/opinion-to-bolster-cybersecurity-the-us-should-look-to-estonia/

Schneier, B. (2003). *Beyond fear*. Springer New York.

Taleb, N. N. (2016). *Antifragile: Things that gain from disorder*. Random House Incorporated.

UK Ministry of Defence [MOD]. (2017). *Wargaming handbook*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

US Department of Homeland Security [DHS]. (2020). *Homeland threat assessment* (Rep.). https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf