Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers

Steven Loleski

To cite this article: Steven Loleski (2019) From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers, Intelligence and National Security, 34:1, 112-128, DOI: 10.1080/02684527.2018.1532627

To link to this article: https://doi.org/10.1080/02684527.2018.1532627

INTELLIGENCE AND NATIONAL SECURITY
2019, VOL. 34, NO. 1, 112–128
https://doi.org/10.1080/02684527.2018.1532627

Routledge
Taylor & Francis Group

ARTICLE

From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers

Steven Loleski

ABSTRACT

How did the National Security Agency (NSA) adopt the practice of hacking? This paper explores how NSA confronted the digital age by focusing on arguably NSA's key organizational innovation as a microcosm of these broader changes: the Office of Tailored Access Operations (TAO). This paper develops a pragmatist model of organizational change showing how the practice of hacking became a practical solution to deal with the problems posed by a globally networked world through TAO's case history. TAO's aggressive expansion by developing a scalable Computer Network Exploitation (CNE) architecture was designed to keep NSA relevant in the twenty-first century.

> *In order to get through the morass of data, we have become, rather than gatherers of the past, hunters in cyberspace.*[1]
>
> – Bill Black, former NSA Deputy Director

Why and how did the National Security Agency (NSA) get into the practice of state-sponsored hacking[2]? Since this change coincided with the winding down of the Cold War and in an era of shrinking budgets, traditional explanations of military innovation stressing military threats or organizational competition seem limited. Craig Wiener's significant study by drawing on an intraservice model of military innovation, by contrast, locates the impetus for Computer Network Operations (CNO) in senior leaders overcoming bureaucratic resistance to push forward a new theory of war.[3] While this intraservice model of innovation captures the bureaucratic manoeuvres necessary to institutionalize innovation, its understanding of where innovation comes from is underdeveloped. The implication here is that new ideas are generated and are delayed in their implementation owing to bureaucratic obstacles. However, this overlooks how changes in the telecommunications environment generated considerable problems for passive signals intelligence (SIGINT) and the early efforts and inquiry aimed at redefining, repurposing, and reorienting action by elements within NSA. In this paper, I develop a pragmatist framework of organizational change that incorporates a fuller understanding of the experimental character of change. A pragmatist account can show how creative innovation to solve problems can reorient action in the face of novel environmental changes. For NSA, this meant that passive interception was no longer a viable option in a changed globally networked world. Tailored Access Operations' (TAO) distant predecessors' efforts against computer network exploitation expanded the mission space and led to reflection at NSA about how the cyber domain was to be another component of SIGINT. While bureaucratic cover mattered in terms of protecting these nascent efforts, the value of a pragmatist perspective is to show how action and inquiry were deeply implicated in shaping this mission area and how the practice of active SIGINT was increasingly seen as a practical solution to NSA's mission enablement. Going further, a pragmatist explanation can explain why these hacking efforts did not

CONTACT Steven Loleski steven.loleski@mail.utoronto.ca

remain boutique experiments but rather expanded into industrial-scale exploitation. TAO's aggressive expansion by developing a scalable CNE architecture was designed to keep NSA relevant in the twenty-first century.

This paper will proceed as follows: first, I will discuss the intraservice model of military innovation and address some of its limitations, before turning to a discussion of the pragmatist theory of action and framework for organizational change. The mechanism of this pragmatist approach will be explored through a case history of NSA's efforts to redefine the SIGINT paradigm to its culmination in the creation and maturation of TAO.

From listening to hacking

The NSA is an element of the US Intelligence Community responsible for collecting, processing, and reporting foreign intelligence and counterintelligence through signals intelligence activities as well as protecting US National Security Systems.[4] While much more is known and discussed about NSA's role in early computer security stemming from its technical expertise,[5] much less attention is explicitly devoted to the remarkable changes in intelligence orientation ushered in by networked computers. Former NSA Director Hayden reflected, 'With little debate, we went from a world of letting radio waves serendipitously hit our antennas to what became a digital form of breaking and entering'.[6] This innovation, as Hayden continued, appeared 'less innocent and less inevitable'[7] to some in the wake of the Snowden disclosures. In this section, I would like to address how NSA's traditional SIGINT and IA missions evolved to enable CNO by drawing on Craig Wiener's substantial case history along with other declassified and unauthorized sources. Wiener highlights the bureaucratic machinations that institutionalized CNO in the United States by focusing on the intellectual and organizational tools key individuals played in creating change.[8] While he captures the bureaucratic politics necessary to institutionalize innovations, the intraservice model cannot adequately understand where those innovations originate nor understand how innovation occurs short of major military doctrine.

Unlike many obvious sources of military innovation spurred by external military threats or defeats in war,[9] the transition to CNO largely occurred in an era ready for a peace dividend. Indeed, Weiner's main theoretical foil is Barry Posen's Civil–Military relations model that broadly points to the external threat environment and major military loss as the source of doctrinal innovation. At various stages, Weiner does not find this convincing given the 'relatively placid' international environment during key developments.[10] Arguments concerning bureaucratic competition over resources, mission, and prestige can also generate innovation.[11] Bureaucratic turf battles have a long history in the Intelligence Community, and in particular between NSA and CIA.[12] While this competition manifested itself over endpoint access or mission relevance, Weiner finds rather than competition 'interagency cooperation between NSA and CIA channeled through the IOTC [Information Operations Technology Center]… led to the maturation of CNE and CNA technologies'.[13] Instead, drawing from Stephen Rosen, Weiner argues that the intraservice model of military innovation is the most persuasive explanation of CNO development. Put simply, visionary leaders using intellectual and organizational resources were able to overcome bureaucratic obstacles to push their vision forward. New theories of victory are important insofar as they 'affect the distribution of power' and help win the '"ideological" struggle that redefines the values that legitimate' the organization.[14]

However, while this perspective sheds light on how innovation can overcome entrenched bureaucratic interests, its understanding of where innovation comes from is underdeveloped. More fundamentally, this owes to Wiener's (and Rosen's) ontological commitment maintaining a strict separation between ideas and action. 'The new theory', Rosen contends, 'must be translated into concrete, new tasks that are performed everyday' because '"ideological" innovations remain abstract and may not affect the way the organization actually behaves'.[15] Peacetime military innovation is a 'slow internal process, effectively stretching across a generation'[16] because of the

'large gap between the intellectual breakthroughs … [and] the initiation of a bureaucratic strategy'.[17] In the case of NSA's transition to endpoint accesses, Director 'McConnell's recognition that NSA would have to live on the Net was known internally for over ten years, although the changes had yet to be made'.[18] As a result, NSA's early 'boutique' efforts with CNE/CNO development are not given analytical weight 'until brought out of the shadows by Bill Black in 1996'.[19] The model of innovation here is that new ideas are generated and are delayed in their implementation owing to bureaucratic obstacles.

However, this undervalues the interim and ongoing process of collective inquiry and situated creativity from 'learning how to move forward under new circumstances that have rendered old understandings obsolete'.[20] In a review of NSA documents dated 1993–1995, NSA's experience displays:

> small measure of 'protecting rice bowls' and other bureaucratic pathology, but overall they reveal men and women confronting something understood only as what it was *not* (e.g., 'this doesn't fit with what we've known as information warfare') and advancing and correcting hypotheses. Personnel wondered if the cyber domain could be, in its 'offensive' dimension, a component of signals intelligence (SIGINT), but generally they were trying to observe and understand before attempting to define.[21]

Nolte's internal review offers a decidedly different interpretation of how innovation unfolds and, in particular, how NSA confronted it. While bureaucratic intransigence was certainly present, there was not a bureaucratic struggle for power over clearly articulated predoctrinal theories of war as Rosen and Wiener would suggest. Instead, the picture that does emerge of the Agency is one confronting a new reality, using past habits to orient action, and beginning to know through doing fragmented 'boutique' efforts organized around specific technological areas. Wiener treats novel ideas, like active SIGINT,[22] as tools wielded by key managers in order to overcome 'partisan interagency intransigence'.[23] While this may occur, the treatment of novel ideas as merely instrumental to promote a new way of war against entrenched bureaucratic legacy programmes cannot understand how these concepts are more appropriately seen as creative innovations and reorientations in response to substantive problem-solving facing practitioners. In the next section, I will discuss a pragmatist account of organizational change before looking specifically as TAO's organizational history.

A pragmatist theory of action

Pragmatism is a philosophical tradition originating with key American thinkers such as Charles Sanders Peirce, William James, and John Dewey.[24] Pragmatist philosophy arose in response to the problem of Cartesian doubt: whether 'our beliefs do (or can) somehow "correspond" to some reality "out there."'[25] Instead, pragmatism anchors 'cognition in real-life problem situations' and the 'search for truth for the purpose of coping with real problems encountered in the course of action'.[26] For Dewey, in particular, 'concrete acts of knowing start off in an interaction situation characterized by a 'transaction taking place between an individual and what, at the time, constitutes his [*sic*] environment'.[27] Our ideas and perceptions are not logically prior to the world and whether they correspond to it but rather our perceptions and ideas are shaped by experience and habits. In other words, the mind and world are 'mutually created by their ongoing interaction'.[28] Over time, a 'cumulative linking of acts that structures experience' form habits. [29] A pragmatist understanding of habit differs from popular conceptions as automatic modes of action. A habit, Dewey suggests, is '"an acquired predisposition to ways or modes of response," which (contingently) manifests in similar though not identical acts across social time and space'.[30] Habits are ways of coping with the problems that inhere in the need to interact with the world. They are socially recognized acts but enacted by individuals rather than bureaucracies or institutions.[31] Institutions can be a form of collective habituation among a community of individuals joined together by shared dispositions and future expectations.

Habits borne through experience provide a reliable way for individuals to solve problems. But in response to 'problem situations', action 'alternates between habit and creativity'.[32] So, while habits stabilize experience and meaning, changes in social and material environments can interrupt our habits that do not conform to our prior experiences or expectations. New situations or 'environmental stimuli' could refer to material or social changes like disruptive or changing technologies or also factors endogenous to social interaction if habits conflict or are contested.[33] 'When the flow of activity of a habit is frustrated by an environment that no longer conforms to the expectations that in part constitute the habit, the actor critically assesses the habit since the action it prescribes is no longer appropriate or possible'.[34] Given that habits are collectively enacted in organizational settings, it is not unreasonable to assume these habits are more engrained and require growing environmental incompatibility. These insights might resemble the concept of 'institutional memory' but for pragmatists institutional memory resides in shared ways of doing things.

When habitual action is confronted with an emerging problem for which experience is ill equipped, actors must reflect on solutions to reorient action. Importantly, our habits form the context for understanding new problems as well as resources for the development of new ones.[35] Pragmatism at its core, Joas explains, is 'a *theory of situated creativity*:'[36]

> For the pragmatists, action consists not in the pursuit of clear-cut goals or in the application of norms, and creativity is not the overcoming of obstacles along these prescribed routes. Anchoring creativity in action allows the pragmatists to conceive of creativity precisely as the liberation of the capacity for new actions.[37]

If individuals succeed in creatively redefining the new action situation, they will have introduced new possibilities for action in the world. Therein lies the potential for human agency or 'the reflexive creativity of socially situated action'.[38] However, the process of forming new habits is not straightforward given the doubt and uncertainty generated by new realities. Any critical appraisal of a habit occurs in a social context where new habits materialize from the process of 'collective reflection, deliberation, and experimentation'.[39] As the world continues to interrupt on our habits; we have to learn to get on under new circumstances.

A pragmatist view of organizational change

Pragmatism is not meant to supplant organizational theories but its understanding of social action can enrich an organizational perspective[40] and specifically, the intraservice model of military innovation. The latter's view of innovation implies that ideas are created by visionary leaders and delayed until bureaucratic fortunes change. While intelligence of foreign powers does not necessarily lead to innovation,[41] broadening the scope of social action concerning problem dilemmas facing actors can more readily explain when and how habits become incongruent with an actor's environment without reifying *ex ante* what those problems are. More fundamentally, however, pragmatism's theory of action suggests that means and ends mutually constitute by showing how an actor's goals can change over time, how new means can create new interests, and how goals are refined as they develop a sense of what is possible.[42] By contrast, Rosen and Wiener's argument that a new theory of war articulates goals that changes action only until bureaucratic pathways are created misses the reciprocal nature of means-ends construction. For pragmatists, bureaucratic lag is not delayed implementation but a crucial part of creative innovation where actors refine their understandings of the means and ends made by possible by a new situational context and the long and uneven process learning to come to terms with a new reality.

A pragmatist explanation would 'view social mechanisms as composed of chains or aggregations of actors confronting problem situations and mobilizing more or less habitual responses'.[43] In other words, pragmatism should explain why and how actors with certain experience when faced with a problem situation reorient themselves in the way they do. The mechanism then should first explain actors' habits, a problem situation that interrupts experience, the situated creativity designed to reorient action, and the settling and maturation of new habits. In the next section, I

briefly review NSA's Tailored Access Operations (TAO) organizational history to highlight the mechanism of change from passive to active SIGINT.

Intelligence habits

Though many definitions of intelligence abound, pragmatists would focus on intelligence as an activity rather than the product of that activity.[44] Recall that the 'primacy of practice – "perhaps *the* central" principle of pragmatism' cannot be understated.[45] SIGINT, in particular, is 'the process of obtaining secret or unknown information from communication systems or signals'.[46] Depending on a researcher's analytical focus, a referent group of actor's can be national leaders vis-à-vis their respective intelligence services as distinct but complementary communities of practice or at a more granular level intelligence professionals themselves in their respective organizational context. For the purposes of this paper, I will focus on the embodied habits of signals intelligence and in particular at the NSA.

Signals intelligence is a 'form of intelligence derived from the collection and processing of various forms of electronically transmitted data and information; those forms being the communication of human intelligence, or COMINT, and data derived from electronic emission devices, primarily radar (electronic intelligence), or ELINT' and in some cases intercepted telemetry or instrumentation information.[47] SIGINT, then, are activities designed to study and collect how signals and data are communicated and what can be divined from those communications or the process itself. Given that signals analysis and development along with other technical intelligence subfields crucially rests on technological trends, there exists a disposition to continually be aware of technologies, communication systems, and how these trends impact mission requirements. SIGINT must continually 'change or die' in response to technologies that constrain action ('those that will complicate our life by making our problems more difficult') and enable action ('those that will offer us increased opportunity for success, provided that we learn them, adopt them, and exploit them').[48] To this end, one should consider 'systems and methods that are now ruled out because of high data-transmission costs will become eminently practical within the next 10 or 15 years. We should start now to think how to use them effectively in solving our new problems'.[49]

SIGINT habits before the digital age are captured by the practice of passive interception of communications. NSA had historically pursued its foreign intelligence mission 'hoping for a transmission' to intercept 'global high frequency communications, shorter-range microwave signals, photons and electrons moving along a cable'.[50] In particular, low power and short-range line-of-sight signals meant that geographic location necessary to intercept these signals mattered. Some of these efforts 'the *Liberty, Pueblo*, EC-121 – resulted in extensive loss of life and property'.[51] Passive interception was a practical solution to the problems of the analogue age given that the target environment against 'dedicated targets' and communications technologies moved slowly.[52] Commercial off-the-shelf products did not really exist and many technologies were developed in-house.

NSA and the Information Age

While effective against the Soviet Union and its allies during the Cold War, SIGINTers facing major technological changes in telecommunications recognized that by 1990 passive interception 'will not be a viable SIGINT position'.[53] These main developments included 'new satellite systems, optical fiber cable, electronic switching, the coalescence of computers and communication nets, and the increasing complexity of telecommunications'.[54] The latter posed especially difficult problems in changing the target environment: 'The most useful data from an intelligence or a SIGINT viewpoint, may be resident in the system in a computer memory, rather than passing over a communication channel. SIGINT, instead of waiting for data to be transmitted and then passively

collecting and exploiting then, will have to penetrate into the nets, find what is there, and extract'.[55] In particular, the rise of personal computing, networked computers, and readily available commercial encryption would change the information and communications environment.[56] As a result of this environmental change, SIGINT professionals were going to be faced with new problems that they did not readily have the tools or skillsets to successfully exploit.

Moreover, the decline of the Soviet Union as a conventional and slow-moving adversary with their own communications systems with the rise of non-traditional targets communicating on the same global network as civilians 'produced enormous stresses on the SIGINT system'.[57] 'By the late 1990s', Director Hayden recounted, 'NSA was well aware that legitimately targetable foreign communications (like those of the Soviet Union's strategic forces) were no longer confined to isolated adversary networks. Modern targets (like Al Qaeda's e-mails on the World Wide Web) were coexisting with innocent and even constitutionally protected messages on a unitary, integrated global communications network'.[58] 'In its forty-year struggle against Soviet Communism', Hayden reflected, 'the N.S.A. was thorough, stable, and focused' and asked, 'what's changed?' he answered, 'All of that'.[59] There was a growing realization that passive collection could not be relied upon to solve the problems of tomorrow.

Wiener recognizes these changes by noting that the 'possibility of future limitations on NSA collection capabilities due to dynamic changes in information and communications technology is a plausible type of *organizational* threat' before suggesting that such expectations are 'congruent with Posen's assertions' and ultimately 'cannot be seen as a substantial factor' driving CNO capabilities.[60] However, it is not altogether clear why this type of 'plausible' organizational threat is not a key factor in NSA's transformation and why the role of senior leaders promoting a 'predoctrinal theory of victory' should be analytically privileged.

Thinking out loud and re-inventing NSA

Faced with uncertainty from a novel and growing telecommunications environment, NSA engaged in a collective process of inquiry, deliberation, and problem solving. It built on past habits of target development to redefine and reorient the cyber realm as a component of SIGINT. Importantly, the origins of this effort and TAO's predecessor's in particular began when small groups were looking for solutions to specific problems posed by different technological areas. Computer exploitation and network activities began at NSA in 1985 from two groups: P04's Feasibility study and B03, respectively.[61] P04's study led to the creation of G08 in 1986 focused on computer exploitation and evolved to G44 to K15 and ultimately to K7. Packet switching network activities originated in B Group and, in particular, B03 evolving to P571 to G08 to G44 to K15 culminating in K732.[62] Though P571 began exploiting packet switching networks, it also developed a PBX effort to exploit these voice systems along with working against central office switches technology in 1989 partnering with CIA.[63] The key point about these early efforts to exploit computers and networks leading to K7 was that groups began 'working a dozen or so technology areas' and 'in other technology areas, they grew from our realization that given a new technology (e.g., ATM, Computer Telephony Integration) we had to be involved'.[64] Former Deputy Director Bill Black recalled 'only one small pocket at NSA was doing it [computer network exploitation]… G Group', which was led by Dennis Chiari. Former Director Ken Minihan had cordoned off a 'couple dozen of the most creative SIGINT operators' to continue developing the tailored access portfolio.[65]

NSA's experience during 1993–1995, reflects the Agency's 'efforts to come to grips with a rapidly changing information environment'.[66] NSA Director McConnell, in 1994, issued a memorandum to 'Define "Information Systems Intelligence" and Designate "INFOSINT" as a component of SIGINT'.[67] At the same time, another briefing document refers to 'COMPUINT'.[68] These concepts reflect the 'fluidity of the problem' NSA confronted but also clearly relying on past habits to re-orient action by integrating this new realm as a part of SIGINT and clearly within NSA's purview.[69] The former chief of G4 writing in the mid-90s claimed that the concepts of Global Network Intelligence (GNI) and Information Warfare

(IW) 'have become part of NSA's language over the past couple of years'.[70] In 1997, the Senate Intelligence Committee's established the Technical Advisory Group (TAG) which issued a scathing report on NSA the following year casting doubt on the Agency's ability to adapt to technological changes. In response to Congressional tasking, NSA's Scientific Advisory Board was assigned to produce a two-part study on NSA's management of conventional and 'C2C' programmes.[71] The report concluded that NSA should have a 'commitment to re-tool: organizationally, programmatically, and technologically' towards a 'universally understood template of the concept of SIGINT'.[72] Profound changes in target and technology trends forecasting approximately 300 per cent growth in the volume of traffic demanded a new SIGINT paradigm.[73] 'Digital Network Intelligence (DNI)', defined as 'the intelligence from intercepted digital data communications transmitted between, or resident on, networked computers', was identified as the new SIGINT concept.[74] DNI was an outgrowth of the earlier 'C2C'[75] concept likely realizing that 'the "computers" become the intelligence "targets" of highest priority'.[76] The report also specified a 'DNI functional taxonomy' organized along conventional lines: 'access and collection, processing and exploitation, analysis and reporting, and dissemination'.[77]

Wiener's emphasis of such early efforts is to show that while they existed, changes did not occur until Bill Black championed Chiari's efforts in 1996. However, a pragmatist account of change would instead begin with the evidence in the case history to show that these early CNE efforts began in response to specific technological areas that presented particular problems. Through these activities, problem solving led to creative innovations as developments on exploiting computers and networks were refined or in other cases led to realizations that NSA must get involved in other technological areas like PBX traffic. Rather than having articulated a 'new theory of victory' lying dormant until Bill Black brought it out of the shadows, these activities clarified the mission space over time and opened up new areas of involvement. These dynamics should not be downplayed but instead shown to be consistent with a pragmatist account stressing the experimental character of change. In other words, theories of victory do not precede action but theories are part of and an outgrowth of action.

More specifically, Wiener highlights the bureaucratic resistance by the old guard at NSA that viewed CNE as a distraction at best and a detriment to NSA's core missions at worst. While this is important and becomes particularly so during Hayden's and Black's reorganization beginning in 1999, a pragmatist account stresses the process of social learning which is at times challenging, uneven, and disruptive. The change from the analogue to the digital world fundamentally 'transformed the concept of signals intelligence, the NSA's stock in trade. SIGINT had long been defined as passively collecting stray electrons in the ether; now, it would involve actively breaking and entering into digital machines and networks'.[78] General Hayden explained:

> At NSA we had to develop a whole new language. We were moving to *active* SIGINT, commuting to the target and extracting information from it, rather than hoping for a transmission we could intercept in traditional *passive* SIGINT. This was all about going to the *end point*, the targeted network, rather than trying to work the *midpoint* of a communication with a well-placed antenna or cable access.
>
> We also knew that if we did this even half well, it would be the golden age of signals intelligence.[79]

Signals intelligence had to be reinvented and reoriented to deal with an emerging world challenging its traditional mission relevance around novel hacking practices. While Wiener focuses on 'warlord' Group leaders resisting this change out of parochial concerns, what is neglected is the sizeable cognitive leap and skill sets required in adjusting to the new world. Paul Baran underscored this point when he described the difficulties of explaining packet switching to AT&T: 'We just weren't on the same wavelength… But it was a mental block. They didn't understand digital. It was mostly generational, but there were young analog guys who had the same problem'.[80] Barbara McNamara, NSA's Deputy Director from 1997 to 2000, was singled out: 'She's leading a cohort of thirty-year veterans who go back to radio and think nothing is needed'.[81] These active SIGINT practices would only become naturalized by the dramatic influx of a new generation of SIGINTers to swell TAO's ranks. By 2010, some members of the workforce lamented that Fort Meade

resembled 'Ocean City West' where 'shorts and flip-flops don't exactly convey the image of a fierce SIGINT warrior'.[82]

By the time Director Hayden entered NSA in 1999, he was moved by the Senate and NSASAB studies along with a memorandum from James Taylor, then-acting Deputy Director of Operations, which all pointed to the problems of NSA's mismanagement in adapting to changing circumstances.[83] Congressional oversight through its Technology Advisory Group (TAG) reports similarly cautioned that '[d]eclining budgets and obsolete equipment are impeding NSA's ability to maintain their technical edge'.[84] Notwithstanding the more alarmist media reporting surrounding the European investigations in Echelon, the EU reports and others had drawn more conservative conclusions about the NSA's capabilities and pointed to the challenges posed by fibre optic cables, encryption, and the growing volume of communications.[85]

As a result, Hayden commissioned two major management studies: one drawn from an outside group of experts and the other comprised of 'responsible anarchists' within the Agency.[86] NSA was a 'misaligned organization' in the midst of a 'leadership crisis for the better part of a decade'.[87] In particular, 'NSA does not have a single, cohesive strategy or implementation plan for SIGINT modernization' and efforts have been 'fragmented and duplicative' especially in the critical mission area of 'Digital Network Exploitation'.[88] The passive or conventional approach to signals intelligence was no longer viable:

> Now, communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia. They are dynamically routed, globally networked and pass over traditional communications means such as microwave or satellite less and less. Today, there are fiber optic and high-speed wire-line networks and most importantly, an emerging wireless environment that includes cellular phones, Personal Digital Assistants and computers. Encryption is commercially available, growing in sophistication, and packaged in off-the-shelf computer software. The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. To perform its offensive and defensive missions, NSA must 'live on the network'.[89]

NSA must maintain a permanent presence of the global network and 'when necessary succeeding through tailored access'.[90] The Signals Intelligence Mission would be organized into three areas: Global Response, Global Network, and Tailored Access.[91] Access was envisioned as the key difference that marked the transition from passive to active SIGINT. Following the conclusions of the reports, Hayden initiated a '100 Days of Change', which lasted from 15 November 1999 to 30 March 2000, to push through some of these recommendations. Trailblazer was named the 'core strategy to exploit the digital net'[92] with the aim of developing an 'architecture that was common across our mission elements, interoperable, and expandable'.[93] While the SIGINT modernization at NSA is multi-faceted, discussing multiple elements is beyond the scope of a single paper and as a result I will focus on the key organizational innovation that changed the concept of SIGINT from passive to active: Tailored Access.

The TAO of hacking

Far from the budgetary, management, and operational constraints of the late 1990s, by 2013, NSA was leading a 'clandestine campaign that embraces the Internet as a theater of spying, sabotage and war'[94] with Edward Snowden suggesting 'whose goal was the elimination of all privacy, globally'.[95] Media reporting has focused almost exclusively on the technical wizardry of TAO and the methods used to undermine global communications and in particular a heightened concern with zero-day exploits.[96] While there are important privacy concerns at stake brought to light, there has been very little in the way of a theoretical framework to contextualize these developments. The pragmatist explanation outlined in this paper with its problem-solving ethos is a useful framework in which to understand TAO's expansion. Specifically, NSA was faced with a problem: terrorists and foreign adversaries could now 'harvest the product of a $3 trillion a year telecommunication industry, an industry that had made communication signals varied, global, instantaneous, complex, and encrypted'.[97] In order for NSA and SIGINT to remain an 'industrial strength source of American

intelligence',[98] NSA would have to rapidly expand TAO and develop infrastructure for global network exploitation. When confronted with the problem of the number and diversity of target communications, NSA innovated to build a large-scale command-and-control architecture and at the operational level with different exploitation methods that would work with that global architecture. The result was that NSA's digital network exploitation efforts would not 'resemble an intelligence boutique – limited product line, limited customer set, and very high unit prices'[99] but strive for global network dominance.

In the newly established SIGINT Directorate, the Office of Tailored Access Operations was set up 'in the last days of 2000', though did not become fully operational until 2002.[100] Hayden noted, 'We had toyed with some boutique end-point efforts below, but this was different. This was going to be industrial strength'.[101] Following 9/11, 'TAO became the fastest-growing part of NSA post-9/11 bar none'.[102] September 11th was the catalyst that enabled TAO's aggressive expansion and accelerated the reinvention effort already championed by General Hayden and NSA's senior leadership. NSA's SIGINT Director Maureen Baginski 'believed and implemented that ["hunters rather than gatherers"] strategy well before September 11th, and then she applied it with a vengeance to Al Qaeda after the attacks'.[103] NSA has historically invested great sums of money and resources to break or subvert the encryption systems of foreign intelligence targets, yet since 9/11 has increasingly relied on a 'new breed' of 'clandestine intelligence activities for much of their success in penetrating foreign communications networks and encryption systems'.[104]

TAO has reportedly been one of the most successful units at NSA post-9/11 by producing valuable intelligence on targets ranging from high-level nation-state rivals to counterterrorism targets.[105] In its early years, TAO was characterized as 'just a bunch of hackers' relying on techniques not unfamiliar to cyber-criminals like 'tempting targets to click on a link in an innocent-looking e-mail'.[106] Yet, in order to build up its ranks and infrastructure to expand endpoint operations, NSA established a Remote Operations Center (ROC) at Fort Meade in 2005 and subsequently stood up TAO outposts across the Regional SIGINT Operations Centers (RSOCs) in Hawaii, Georgia, Texas, and Colorado. TAO's dramatic growth was built from an 'incredible cohort of young, technically talented, innovative, and adventurous new SIGINTers'.[107] In other words, 'hackers, geeks, and nerds!'[108] A member of TAO reflected on the casual working environment with a very 'DEF CON feel to the place'.[109] Many employees attend the annual hacker convention DEF CON and share 'a similar mindset of wanting to tear things apart, to dig in, to see how things work'.[110] In 2012, NSA Director Keith Alexander dressed in jeans and a black t-shirt gave a keynote address at the convention.[111] These dispositions surely inform TAO's 'no target impossible to penetrate' ethos and 'getting the ungettable' is how NSA describes the unit.[112]

TAO's expansion towards global network dominance

NSA's GENIE Project oversees TAO's endpoint activities designed to 'actively subvert systems that create, store, or manage information – computers, peripherals, and telephone switches – in order to directly retrieve data of intelligence value'[113] 'GENIE Endpoint activities use surreptitious virtual or physical access to create and sustain a presence inside targeted systems and facilities'.[114] TAO's endpoint activities largely rest on obtaining remote access via covert implants and infrastructure throughout the world. In 2004, NSA was managing about 100–150 implants worldwide to 21,252 by 2008 and was projected to control 85,000 by the end of 2013.[115] However, NSA was realizing that managing a global network presence was becoming increasingly difficult and by 2009 it sought to develop an 'intelligent command and control capability' codenamed TURBINE that enables 'industrial-scale exploitation' by automating control of groups of implants.[116] Though the Agency aspired to infect 'millions' of computers, the numbers were in the tens of thousands between 2008 and 2013. It is 'likely to be the case that the Five Eyes need to rely less on network penetrations' owing to their 'tremendous passive collection capability from the core routers and switches of the internet'.[117] CNE might, in other words, play a key role in opening networks that

would enable passive collection to achieve active–passive integration. An internal presentation defines the purposes of 'shaping' as 'taking traffic that normally wouldn't normally go through one of our passive links, and *making* it go through one of our passive links'.[118] Network shaping is an example of an innovative practice designed to address the problem of getting access to traffic you can passively collect.

The GENIE platform architecture NSA has developed to oversee their industrial-sized CNE programmes can also be creatively leveraged to enable network defence and attack. A unit within TAO codenamed Transgression is tasked to 'trace foreign cyber attacks, observe and analyze them and, in the best case scenario, to siphon off the insights of competing intelligence agencies' in a form of cyber counterintelligence.[119] In response to a tip from NSA's defence-oriented National Threat Operations Center (NTOC) about a series of Chinese intrusions in 2009 codenamed BYZANTINE RAPTOR, TAO was able to target and exploit the command and control node of the attackers.[120] NSA hackers were able to extract 'concrete forward-looking defensive value' including information about the source code and tools used by the Chinese. NTOC had the advantage of being 'hot-wired into a vast global SIGINT system that could send scouts out beyond the perimeter to identify activity and threats long before they hit the local firewall'.[121] Despite concerns that NSA has privileged offense over defence, endpoint operations can pay security dividends for national security systems that NSA is authorized to protect under NSD 42.[122] But NSA was also able to access data from other Chinese attacks on UN targets – '[i]n effect NSA is able to tap into Chinese SIGINT collection', – a practice known internally as 'Fourth Party collection'. This is one example to highlight how pragmatism's focus on situated creativity can explain how defensive cleverness can lead to opportunities for further creative action like Fourth Party collection practices or even offensive attacks.[123]

At the operational level, working with Requirements and Targeting analysts and planners, TAO can identify targets of interest based on digital identifiers like 'certain email addresses or website cookies set on a person's computer'.[124] When a target's web communications pass through NSA's passive sensor architecture, TURMOIL, the system tips NSA's centralized active command and control implant architecture, TURBINE, to redirect the target's request by 'briefly hijack[ing] connections between a specific target and a web connection in order to redirect the target to a TAO server (FOXACID) for implantation'.[125] TAO's man-on-the-side CNO capabilities, QUANTUMTHEORY, shoot a response to the target in an effort to beat the response from the legitimate server redirecting to TAO's servers where a malicious payload can be implanted. As an internal presentation makes clear, 'there is more than one way to QUANTUM' meaning that different QUANTUM attacks are designed for different applications like targeting terrorist websites (QUANTUMINSERT since 2005), attacking bot nets (QUANTUMBOT since 2007), to Facebook (QUAUNTUMHAND since 2010), LinkedIn,[126] and even attempted to explore the possibility of identifying some Tor users through QUANTUMCOOKIE.[127] Once exploited, TAO would have 'access to system functions as well as data'.[128] The modularity of the QUANTUM attack suite demonstrates operational innovations to find diverse targets in a global, complex telecommunications environment. For example, while Tor enables anonymous communications and privacy for users, this same platform makes it more difficult for NSA to track the communications of foreign targets.[129] As a result, TAO must look for inventive ways to track Tor users like finding vulnerabilities in Firefox plug-ins.[130] In some cases where remote access is not possible, physical access through supply-chain interdiction is used to install TAO beacon implants by intercepting shipments of network equipment in order to 'pre-position access points into hard target networks around the world'.[131] These techniques have historically been a part of intelligence tradecraft and arguably demonstrate how old habits can be re-oriented to fit new circumstances.

Beyond individual targets, entire networks and network equipment are valuable targets given many devices are connected to a network. TAO has a catalogue describing ways to break into common brands and models of 'routers, switches and firewalls from multiple product vendor lines'.[132] The implants have the ability to persist through software upgrades, to 'copy stored

data, "harvest" communications and tunnel into other connected networks'.[133] According to the *New York Times*, beginning in 2007, Operation Shotgiant sought to exploit China's Huawei network equipment because their global market reach means, 'many of our [NSA's] targets communicate over Huawei-produced products'.[134] Other reporting has similarly confirmed that NSA targets Juniper, Dell, and Cisco network and end-user devices.[135] These software implants can be embedded on a computer's BIOS firmware making it resilient against software updates and unbeknownst to users. Establishing surreptitious persistence on a network allows TAO operators to map networks gaining valuable intelligence but can also enable other defensive and offensive activities.

In 2015, Kaspersky Labs identified an Advanced Persistent Threat (APT) actor dubbed the Equation Group active since at least 2001 and even as early as 1996. The 'suite of surveillance platforms, which they call EquationLaser, EquationDrug and GrayFish, make this the most complex and sophisticated spy system uncovered to date'.[136] The tools and other circumstantial evidence from the Snowden documents link the Equation Group to NSA.[137] These hacking tools, including one later revealed as EternalBlue, provided 'unreal' intelligence collection and were potentially so dangerous that they were debated internally whether the vulnerability should be disclosed to Microsoft according to officials.[138] NSA must weigh risks when deciding to keep vulnerabilities secret against the intelligence value they provide. In August 2016, a group known as The Shadow Brokers purported to have information on hacking tools tied to the Equation Group and began to release a cache of exploits. Some of these exploits, stolen allegedly from NSA, were repurposed by cybercriminals behind the globally disruptive WannaCry ransomware attack and later NotPetya in 2017. Microsoft President, Brad Smith, likened the incident to 'the U.S. military having some of its Tomahawk missiles stolen'.[139] Following WannaCry and NotPetya, there were increased demands that NSA disclose all vulnerabilities. NSA claims it discloses 90 per cent of vulnerabilities to vendors, but disclosing all would be tantamount to 'unilateral disarmament'.[140] The tension here is that NSA and its focus are using vulnerabilities for national security purposes and not all end users, so its focus must remain on finding, keeping, and safeguarding some of them.

Lawful hacking

This paper has largely explored the changing role of technology as it has both affected and enabled NSA's re-orientation to hacking. However, while it may be worthwhile to note that changing norms and laws also affect the possibilities for action, its absence from this discussion largely owes to the fact that there are relatively few constraints and congressional scrutiny on NSA's foreign intelligence activities compared to domestic ones.[141] NSA's foreign intelligence mandate is governed by EO 12333, which authorizes operations in accordance with foreign intelligence purposes and in accord with US laws and regulations protecting privacy (namely, an internal directive translated for SIGINT operations called USSID 18). There is evidence in NSA's Digital Network Intelligence training that analysts are advised to consider USSID 18 and host country protections when targeting. Having said that, the practice of hacking for foreign intelligence purposes was met with little debate or normative re-orienting. As DIRNSA Hayden explains, 'we pretty much had all we needed to thrive, at least in terms of law and policy' and marvelled 'how easily we transferred our system of governance from the old world to the new'.[142] NSA remarkably, yet silently, 'went from a world of letting radio waves serendipitously hit our antennas to what became a digital form of breaking and entering'.[143] However, the broader normative and legal context may be changing with public awareness as Internet routing increasingly blurs the traditional foreign/domestic distinction governing intelligence activities. While NSA relies on the law prohibiting intentionally targeting US persons, there have been concerns raised about US person data incidentally collected abroad or even hypothetically 'shaping' US domestic communications for foreign collection.[144] Given the secrecy surrounding such activities, it is difficult to say how these legal and normative questions are navigated or deliberated internally.

We see much more normative and legal transformation moving from hacking to attacking despite knowing that 'defense, exploitation, and attack were technologically and operationally indistinguishable'.[145] Getting offensive cyber operations off the ground meant some 'unwieldy' or innovative institutional blending: 'Fort Meade would access and conduct reconnaissance of a target based on my authorities as DIRNSA and then, on order, could manipulate or destroy the target based on [Gen.] Cartwright's exercising his combat authority through me'.[146] The practice of dual-hatting is a way to navigate the normative and legal thicket of Title 10-Title 50 debates on cyber operations.

Conclusions

This paper has attempted to explore why and how the NSA developed the practice of hacking through its Tailored Access Operations. While Craig Wiener's account of the rise of CNO operations provides a rich case history of related developments, the instraservice approach does not adequately understand the sources of innovation short of major military doctrinal changes. In particular, it is not clear why organizational threats are not seen as significant factors in the case history. In contrast, this paper has drawn from pragmatist sociology to show how creative innovation to solve problems can reorient action in the face of novel environmental changes. For NSA, this meant that passive interception was no longer a viable option in a changed globally networked world. TAO and its fragmented predecessors' efforts were designed to develop an active approach to SIGINT by gaining access to networks. However, the problem faced by NSA was how to scale this new practice given increasing technical, operational, and customer demands. NSA's response was to aggressively expand TAO by developing a global architecture and tools that can augment its traditional passive collection capabilities. The difficulties with implementing these sweeping changes at NSA were not entirely based on parochial resource concerns as Wiener suggests but the conventional ways of passive SIGINT intercepting radio made it difficult for some to understand how the digital world was upending the traditional mission space.

Since the Snowden disclosures and Shadow Brokers, there has been increased attention on NSA and TAO in particular. While media reporting tends to sensationalize the tools and techniques, a theoretical framework is needed to more generally contextualize the growth and expansion of TAO. In particular, pragmatism's problem-solving ethos helps us understand how the scope and scale of CNE at NSA has matured as a way to aggressively keep the Agency relevant in a complex, global telecommunications environment. Both at the infrastructure level and the operational level, TAO has sought to innovate to address the problems and opportunities posed by industrial-scale exploitation. Future work could develop the argument further by showing how TAO's hacking efforts have been and can be used for both defensive and offensive means in greater depth.

Notes

1. Lardner, "After 40 Years at NSA."
2. This paper uses the term hacking and Computer Network Exploitation (CNE) interchangeably defined as 'enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks' (see Joint Publication 1–02).
3. Wiener, "Penetrate, Exploit, Disrupt, Destroy."
4. Both of these authorities can be found in Executive Order (EO) 12333 and National Security Directive (NSD) 42, respectively.
5. Warner, "Cybersecurity"; and Johnson, "American Cryptology."
6. Hayden, *Playing to the Edge*, 141.
7. Ibid., 142.
8. See note 3 above.
9. Posen, *The Sources of Military Doctrine*.
10. Wiener, "Penetrate, Exploit, Disrupt, Destroy," 256.
11. Huntington, "Interservice Competition"; and Downs, "Inside Bureaucracy."

12. Johnson, "American Cryptology."
13. Wiener, "Penetrate, Exploit, Disrupt, Destroy," 336.
14. Rosen, *Winning the Next War*, 20.
15. Ibid., 20.
16. Wiener, "Penetrate, Exploit, Disrupt, Destroy," 331.
17. Rosen, *Winning the Next War*, 81.
18. Wiener, "Penetrate, Exploit, Disrupt, Destroy," 137.
19. Ibid., 173.
20. Schmidt, "Foreign Military Presence," 821.
21. Nolte, "Anticipating Cyberspace Security," 27.
22. Hayden, *Playing to the Edge*.
23. Wiener, "Penetrate, Exploit, Disrupt, Destroy," 340. As Wiener suggests, major military innovations 'clearly should have an empowered champion with significant intellectual capacity and a variety of hard and soft skills'.
24. Menand, *The Metaphysical Club*.
25. Hellmann, "Beliefs as Rules for Action," 640.
26. Joas, *The Creativity of Action*, 128.
27. Jackson, "Situated Creativity," 657.
28. Hildebrand, *Dewey*, 21.
29. Ibid., 23.
30. Pratt, "Pragmatism as Ontology," 6.
31. Schmidt, "Foreign Military Presence," 819.
32. Gross, "A Pragmatist Theory."
33. Schmidt, "Foreign Military Presence," 820.
34. Ibid., 820.
35. Ibid., 820.
36. Joas, *The Creativity of Action*, 133; Jackson, "Situated Creativity'. For a theory developing a mechanism of creative innovation, see Emanuel Adler, "International Social Orders," forthcoming.
37. Joas, *The Creativity of Action*, 133.
38. Pratt, "Pragmatism as Ontology," 13.
39. Schmidt, "Foreign Military Presence," 821.
40. Lorino, *Pragmatism and Organization Studies*; and Farjoun, Ansell, and Boin, "Perspective – Pragmatism in Organization Studies."
41. Rosen, *Winning the Next War*.
42. Pratt, "Pragmatism as Ontology," 14; and Joas, *The Creativity of Action*.
43. Gross, "A Pragmatist Theory," 368.
44. Warner, "Wanted," 18.
45. Hellmann, "Beliefs as Rules for Action," 639.
46. Meyer, "SIGINT," 14.
47. Nolte, "Signals Intelligence," 81.
48. Raymond, "Challenge to Sigint," 11.
49. Ibid., 13.
50. Hayden, *Playing to the Edge*, 133–34.
51. Redacted, "Ground-Based Remote Intercept," 5.
52. Nolte, "Signals Intelligence."
53. Redacted, "SIGINT," 18.
54. Meyer, "SIGINT," 13.
55. See note 53 above.
56. Nolte, "Signals Intelligence," 105.
57. Ibid., 106.
58. Hayden, *Playing to the Edge*, 405.
59. Hersh, "The Intelligence Gap."
60. Wiener, "Penetrate, Exploit, Disrupt, Destroy," 257.
61. Redacted, "The K 7 Story."
62. Ibid., 7.
63. Ibid.
64. Ibid.
65. Kaplan, *Dark Territory*, 134.
66. Nolte, "Anticipating Cyberspace Security," 36.
67. Ibid., 29.
68. Ibid., 30.

69. Nolte, "Signals Intelligence," 30.
70. Redacted, "Global Network Intelligence and Information Warfare," 29. Also, Information Warfare treated 'the global network from a different perspective than GNI' (34). Information Warfare, Operations and the inter-agency IOTC are beyond the scope of this paper. These developments are more directly addressed by Wiener, "Penetrate, Exploit, Disrupt, Destroy."
71. Clapper and NSA Scientific Advisory Board, "Digital Network Intelligence (DNI), Report to the Director."
72. Ibid.
73. Ibid.
74. Ibid., 20.
75. See note 71 above.
76. Black, "Thinking Outloud About Cyberspace," 4.
77. See note 71 above.
78. Kaplan, *Dark Territory*, 132.
79. See note 22 above.
80. Brand, "Founding Father." I thank a participant at the International Studies Association Annual convention for this reference.
81. Hersh, "The Intelligence Gap."
82. Redacted and National Secuity Agency/Central Security Agency, "Dress Code."
83. Taylor, "Thoughts on Strategic Issues for the Institution."
84. "Special Report of the Select Committee," 34.
85. Richelson, "Desperately Seeking Signals."
86. Bamford, *Body of Secrets*, 470.
87. New Enterprise Team, "(NETeam) Recommendations."
88. Ibid., 20.
89. National Secuity Agency/Central Security Service, "Transition 2001," 31.
90. Ibid., 31.
91. External Team Report, "A Management Review for the Director."
92. Hayden, "DIRgram-122."
93. Hayden, *Playing to the Edge*, 20.
94. Gellman and Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations."
95. Greenwald, *No Place to Hide*, 47.
96. Healey, "The U.S. Government and Zero-Day Vulnerabilities."
97. "Testimony From the Joint Intelligence Committee."
98. Ibid.
99. Ibid.
100. Hayden, *Playing to the Edge*, 134; and Wiener, "Penetrate, Exploit, Disrupt, Destroy," 235.
101. Ibid., 134.
102. Ibid., 134.
103. See note 97 above.
104. Aid, "The NSA's New Code Breakers."
105. Aid, *The Secret Sentry*, 301.
106. Redacted, "Interview with a SID 'Hacker' – Part 1"; and Hayden, *Playing to the Edge*, 135.
107.. Hayden, *Playing to the Edge*, 135.
108. Redacted, "Interview with a SID 'Hacker' – Part 2."
109. Redacted.
110. Ibid.
111. Mills, "NSA Director Finally Greets Defcon Hackers."
112. See note 107 above.
113. Redacted, "Expanding Endpoint Operations"; Appelbaum et al., "The Digital Arms Race"; Gellman and Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show – The Washington Post."
114. Appelbaum et al., "The Digital Arms Race."
115. Gallagher and Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware"; and Gellman and Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show."
116. Gallagher and Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware."
117. Buchanan, *The Cybersecurity Dilemma*, 68.
118. Intercept, "Network Shaping 101," 27.
119. See note 114 above.
120. NSA/CSS Threat Operations Center (NTOC) Hawaii, "(U//FOUO) NSA's Offensive and Defensive Missions."
121. See note 6 above.
122. I thank Chris Parsons on this point.

123. See note 6 above.
124. Der Spiegel, "The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks."
125. Redacted, "DGO Enables Endpoint Implants via Quantumtheory."
126. Spiegel Staff, "Quantum Spying."
127. Schneier, "Attacking Tor"; and Goodin, "How the NSA Might Use Hotmail, Yahoo or Other Cookies to Identify Tor Users."
128. See note 94 above.
129. Clapper, "DNI Statement"
130. Schneier, "Attacking Tor."
131. Redacted, "Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets."
132. See note 128 above.
133. See note 94 above.
134. Sanger and Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat – The New York Times."
135. Appelbaum, Horchert, and Stöcker, "Catalog Reveals NSA Has Back Doors for Numerous Devices."
136. Zetter, "Suite of Sophisticated Nation-State Attack Tools Found With Connection to Stuxnet."
137. Zetter.
138. Nakashima and Timberg, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did."
139. Apuzzo and Becker, "Trove of Stolen Data."
140. Ledgett, "No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession."
141. Edgar, *Beyond Snowden*.
142. See note 6 above.
143. Ibid.
144. Arnbak and Goldberg, "Loopholes for Circumventing the Constitution."
145. Hayden, *Playing to the Edge*, 143.
146. Ibid.

Acknowledgments

I would like to thank Emanuel Adler, Ronald Deibert, Jon Lindsay, Christopher Parsons, and participants at the annual International Studies Association conference for their helpful comments and suggestions.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Steven Loleski is a PhD Candidate in the Department of Political Science at the University of Toronto. His research broadly focuses on cyber-intelligence, intelligence cooperation, and the relationship between secrecy and democracy. His dissertation explores the resilience of the Five Eyes partnership.

Bibliography

Aid, M. M. *The Secret Sentry : The Untold History of the National Security Agency*. New York: Bloomsbury Press, 2009.

Aid, M. M. "The NSA's New Code Breakers." *Foreign Policy* (blog). Accessed September 13, 2018. https://foreignpolicy.com/2013/10/15/the-nsas-new-code-breakers/.

Appelbaum, J., A. Gibson, C. Guarnieri, A. Müller-Maguhn, L. Poitras, M. Rosenbach, L. Ryge, H. Schmundt, and M. Sontheimer. "The Digital Arms Race: NSA Preps America for Future Battle." *Spiegel Online*, January 17, 2015, sec. International. http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

Appelbaum, J., J. Horchert, and S. Christian. "Catalog Reveals NSA Has Back Doors for Numerous Devices." *Der Spiegel*, December 29, 2013. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Apuzzo, M., S. Shane, and J. Becker. "Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools." *The New York Times*, October 19, 2016. https://www.nytimes.com/2016/10/20/us/harold-martin-nsa.html.

Arnbak, A., and S. Goldberg. "Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad." *SSRN Scholarly Paper*. Rochester, NY: Social Science Research Network, 2015. https://papers.ssrn.com/abstract=2460462.

Bamford, J. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. Reprint edition. New York: Anchor, 2002.

Black, W., Jr "Thinking Outloud About Cyberspace." *Cryptolog* XXIII, no. 1 (Spring, 1997): 1–4.

Brand, S. "Founding father." *WIRED*, March 1, 2001. https://www.wired.com/2001/03/baran/.

Buchanan, B. *The Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System*. Oxford University Press. Accessed October 12, 2017 https://www.amazon.co.uk/Cybersecurity-Dilemma-Network-Intrusions-International/dp/1849047138.

Clapper, J. "DNI Statement: Why the Intelligence Community…." *IC ON THE RECORD*, October 4, 2013. http://icontherecord.tumblr.com/post/63103784923/dni-statement-why-the-intelligence-community.

Clapper, Lt .Gen. Jim, and NSA Scientific Advisory Board. *Digital Network Intelligence (DNI), Report to the Director*. June 28, 1999.

Der Spiegel. "The NSA Uses Powerful Toolbox in Effort to Spy on Global Networks." *Der Spiegel*, December 29, 2013. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

Downs, A. "Inside Bureaucracy." Product Page, 1967. https://www.rand.org/pubs/commercial_books/CB156.html.

Edgar, T. H. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, D.C: Brookings Institution Press, 2017.

External Team Report. *A Management Review for the Director, NSA*. October 22, 1999.

Farjoun, M., C. Ansell, and A. Boin. "PERSPECTIVE—Pragmatism in Organization Studies: Meeting the Challenges of a Dynamic and Complex World." *Organization Science* 26, no. 6 October 7 (2015): 1787–1804. doi:10.1287/orsc.2015.1016.

Gallagher, R., and G. Greenwald. "How the NSA Plans to Infect 'Millions' of Computers with Malware." *The Intercept* (blog), March 12, 2014. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

Gellman, B., and E. Nakashima. "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show – the Washington Post." *The Washington Post*. Accessed September 15, 2018. https://www.washingtonpost.com/.

Goodin, D. "How the NSA Might Use Hotmail, Yahoo or Other Cookies to Identify Tor Users." *Ars Technica*, October 7, 2013. https://arstechnica.com/information-technology/2013/10/how-the-nsa-might-use-hotmail-or-yahoo-cookies-to-identify-tor-users/.

Greenwald, G. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. 1st ed. Toronto: Signal, 2014.

Gross, N. "A Pragmatist Theory of Social Mechanisms." *American Sociological Review* 74, no. no. 3 June 1 (2009): 358–379. doi:10.1177/000312240907400302.

Hayden, M. "DIRgram-122: 'Trailblazer Acquisition Strategy'." September 18, 2000.

Hayden, M. V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Press, 2016.

Healey, J. "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers." *SIPA Journal of International Affairs* 1 (2016): 1–20.

Hellmann, G. "Beliefs as Rules for Action: Pragmatism as a Theory of Thought and Action." *International Studies Review* 11, no. 3 (2009): 638–641. doi:10.1111/j.1468-2486.2009.00889.x.

Hersh, S. "The Intelligence Gap: How the Digital Age Left Our Spies Out in the Cold." *The New Yorker*, December 6, 1999.

Hildebrand, D. L. *Dewey: A Beginner's Guide*. Oxford: Oneworld, 2008. https://search.library.utoronto.ca/details?7037447.

Huntington, S. P. "Interservice Competition and the Political Roles of the Armed Services." *The American Political Science Review* 55, no. 1 (1961): 40–52. doi:10.2307/1976048.

The Intercept. "Network Shaping 101." 2016. https://www.documentcloud.org/documents/2919677-Network-Shaping-101.html.

Jackson, P. T. "Situated Creativity, Or, the Cash Value of a Pragmatist Wager for IR." *International Studies Review* 11, no. 3 (2009): 638–662.

Joas, H. *The Creativity of Action*. 1st. Translated by Jeremy Gaines and Paul Keast, Chicago, IL: University Of Chicago Press, 1996.

Johnson, T. "American Cryptology during the Cold War, 1945–1989." *Center for Cryptologic History* (1995). http://nsarchive.gwu.edu/NSAEBB/NSAEBB260/nsa-1.pdf.

Kaplan, F. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.

Lardner, R. "After 40 Years at NSA, Bill Black Is SIGINT World's Agent for Change." *InsideDefense.com*, July 4, 2002. https://insidedefense.com/inside-pentagon/after-40-years-nsa-bill-black-sigint-worlds-agent-change.

Ledgett, R. "No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession." *Lawfare*, August 7, 2017. https://www.lawfareblog.com/no-us-government-should-not-disclose-all-vulnerabilities-its-possession.

Lorino, P. *Pragmatism and Organization Studies*. Oxford, New York: Oxford University Press, 2018.

Menand, L. *The Metaphysical Club*. 1st pbk ed. New York: Farrar, Straus and Giroux, 2002.
Meyer, J. "SIGINT: 1990 Part 1." *Cryptolog* IX, no. 9 (September, 1982): 1–29.
Mills, E. "NSA Director Finally Greets Defcon Hackers." *CNET*, July 27, 2012. https://www.cnet.com/news/nsa-director-finally-greets-defcon-hackers/.
Nakashima, E., and C. Timberg. "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did." *Washington Post*, May 16, 2017. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.
National Secuity Agency/Central Security Service. "Transition 2001." December 2000.
New Enterprise Team. "(Neteam) Recommendations: The Director's Work Plan for Change." October 1, 1999.
Nolte, W. "Anticipating Cyberspace Security: NSA's Experience, 1992–1997." *Cryptologic Quarterly* (2012): 26–37.
Nolte, W. "Signals Intelligence." *The Five Disciplines of Intelligence Collection*, edited by M. M.Lowenthal and R. M. Clark, 1st 81–110. Thousand Oaks, CA: CQ Press, 2015.
NSA/CSS Threat Operations Center (NTOC) Hawaii. "(U//FOUO) NSA's Offensive and Defensive Missions: The Twain Have Met." *SID Today*, April 26, 2011.
Posen, B. R. *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*. Cornell Studies in Security Affairs. Ithaca, NY: Cornell University Press, 1986.
Pratt, S. "Pragmatism as Ontology, Not (Just) Epistemology: Exploring the Full Horizon of Pragmatism as an Approach to IR Theory." *International Studies Review* 18, no. 3 (September, 2016): 508–527. doi:10.1093/isr/viv003.
Raymond, R. "Challenge to Sigint: Change or Die." *Cryptologic Spectrum* 1, no. 1, (Fall 1969): 11-13.
Redacted. "DGO Enables Endpoint Implants via Quantumtheory." *Special Source Operations News* (blog), September 26, 2011. https://edwardsnowden.com/2017/06/26/dgo-enables-endpoint-implants-via-quantumtheory/.
Redacted, A. "Ground-Based Remote Intercept in the Far East." *Cryptologic Spectrum* 4, no. 2 (Spring, 1974): 5–10.
Redacted, A. "SIGINT: 1990 Part 3." *Cryptolog* IX, no. 11 (November, 1982): 1–29.
Redacted, A. "Global Network Intelligence and Information Warfare: SIGINT and INFOSEC in Cyberspace." *Cryptolog* XXI, no. 1 (1995): 29–38.
Redacted, A. "The K 7 Story - The First 12 Years." *National Security Agency*, December 1998.
Redacted, A. "Expanding Endpoint Operations." *SID Today*, September 17, 2004.
Redacted, A. "Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets." *SID Today*, June 2010.
Redacted, A. "Interview with a SID 'Hacker' – Part 1: How Does TAO Do Its Work?" *SID Today*, July 12, 2012.
Redacted, A. "Interview with a SID 'Hacker' – Part 2: Hacker Culture and Worker Retention." *SID Today*, July 13, 2012.
Redacted, Author, and National Secuity Agency/Central Security Agency. "Dress Code." *Ask Zelda* (blog), June 15, 2010.
Richelson, J. "Desperately Seeking Signals." *Bulletin of the Atomic Scientists* 56, no. 2 March 1 (2000): 47–51. doi:10.2968/056002013.
Rosen, S. P. *Winning the Next War: Innovation and the Modern Military*. Ithaca, NY: Cornell University Press, 1994.
Sanger, D., and N. Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat - the New York Times." *The New York Times*, March 22, 2014. https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?hp.
Schmidt, S. "Foreign Military Presence and the Changing Practice of Sovereignty: A Pragmatist Explanation of Norm Change." *American Political Science Review* 108, no. 4 (November, 2014): 817–829. doi:10.1017/S0003055414000434.
Schneier, B. "Attacking Tor: How the NSA Targets Users' Online Anonymity." *The Guardian*, October 4, 2013, sec. US news. https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.
"Special Report of the Select Committee on Intelligence, January 7, 1997 - October 21, 1998." *Senate Report*. 106–113, February 3, 1999. https://www.intelligence.senate.gov/publications/committee-activities-special-report-select-committee-intelligence-january-7-1997.
SPIEGEL Staff. "Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers." *Spiegel Online*, November 11, 2013, sec. International. http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html.
Taylor, J. R. "Thoughts on Strategic Issues for the Institution." *United States Government memorandum*, April 9, 1999.
"Testimony from the Joint Intelligence Committee - the New York Times." Accessed September 13, 2018. https://www.nytimes.com/2002/10/17/politics/testimony-from-the-joint-intelligence-committee.html.
Warner, M. *Wanted: A Definition of Intelligence*. Washington DC: Central intelligence agency, Center for the study of intelligence, 2002.
Warner, M. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. 5 (October 1, 2012): 781–799.
Wiener, C. *Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation*. George Mason University, 2016. http://search.proquest.com/docview/1864633371/.
Zetter, K. "Suite of Sophisticated Nation-State Attack Tools Found with Connection to Stuxnet." *Wired*, February 16, 2015. https://www.wired.com/2015/02/kapersky-discovers-equation-group/.