Fall 2019

The Morris Worm: Cyber Security, Viral Contagions, and National Sovereignty

Roman Shemakov , '20

The Morris Worm: Cyber Security, Viral Contagions, and National Sovereignty

Roman Shemakov[1]
Swarthmore College

This paper analyzes the history of cybercrime rhetoric through the 1989 hacking of the earliest internet network, ARPANET. The event is useful for understanding how contagion rhetoric of the computer science professionals imprints onto the public consciousness, security agencies, and legal institutions. By drawing on notes from the meetings of the National Computer Security Center, Congressional Hearings, Court Cases, and National Legislation in the aftermath of the Morris Worm, the author explores how contagion discourse constructs protectorate institutions in its image. From the birth of the computing industry in World War II, to the Computer Eradication Act of 1989, this paper traces how popular catastrophic events, like the Morris Worm, construct a public reaction that instinctually abdicates intellectual authority to an expert-induced panic.

Keywords*: internet governance, computer rhetoric, viruses*

A watershed moment for the history of the internet occurred at 11:28 pm on November 2nd, 1988. Academics at Stanford, RAND, MIT, and Berkeley reported that all of their computers stopped operating and they couldn't access any of the information. Within two days, more than 10% of computers in the United States lost functionality. What turned out to be a line of code capable of replicating and moving between systems was difficult to imagine, let alone explain to an American public seldom familiar with the existence of the internet. The code's author, Robert Morris, was a 22 year old Cornell graduate student at the time when he accidentally released the

[1] Author's Note: This paper has benefited from comments by Megan Brown and Bruce Dorsy. I'm especially grateful for all of the technical advice I received from Vasanta Chaganti, Sarah Elichko, and Timothy Burke, as well as all of the inspirational support from Libby Hoffenberg and Jia Chern.

program that would permanently change the way the American public imagined the internet. In an internal investigation, a commission at Cornell University used an analogy emblematic of an incident that lacked any established vernacular or reference point: "a more apt analogy would be the driving of a golf cart on a rainy day through most houses in a neighborhood. The driver may have navigated carefully and broken no china, but it should have been obvious to the driver that the mud on the tires would soil the carpets and that the owners would later have to clean up the mess."[2]

For decades before the Morris Worm was released, the internet was predicted to be an unimaginable revolutionary invention. A 1964 article titled "The Computers of Tomorrow," articulated a future where computerized applications could be applied to "information retrieval, bill payments, and stock trading."[3] Computing promised to be a giant leap forward. But few envisioned it becoming a domain primarily defined by insecurity. Computing is especially fascinating for understanding how cultural knowledge is packaged into artifacts that take on roles of objectivity and reliability.[4] A few historians have done a fantastic job of exploring how Cold War anxieties, political visions, and the AIDS epidemic have been infused into the foundational myths of these machines.[5] I build on the theoretical structure of these works by specifically focusing on the history of the internet and how social symbols get transferred from one cultural domain to another. This paper traces how metaphors of disease and contagion spill out of insular expert laboratories and permanently imprint themselves onto institutions.

---

[2] Ted Eisenberg, D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, and T. Santoro. "The Cornell Commission: on Morris and the Worm." *Communications of the ACM* 32, no. 6 (January 1989): 706–709, 708.
[3] Martin Campbell-Kelly, and Daniel D. Garcia-Swartz. "The History of the Internet: The Missing Narratives." *SSRN Electronic Journal*, 2005, 21.
[4] Stefan Helmreich. "Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism." *Science, Technology, & Human Values* 25, no. 4 (2000): 472–91, 473.
[5] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*. New York: ACLS History E-Book Project, 2005. and Bryan Pfaffenberger. "The Social Meaning of the Personal Computer: Or, Why the Personal Computer Revolution Was No Revolution." *Anthropological Quarterly* 61, no. 1 (1988).

The 1980s became the decade when the promise of an unabated and free telecommunication network was thwarted by the construction of legislative and bureaucratic walls. Rather than considering the internet an inherently revolutionary technology, I build on the work of technology historians by analyzing how computing came to express existing social structures of the 1980s.[6] By considering the history of the internet as a culmination of expectations about security, disease, and the Cold War political logic, it is possible to begin deciphering why cyberspace came to be acknowledged as inherently threatening.[7]

This paper places the Morris Worm -- the first large scale internet attack -- center stage. By beginning with the relationship of the computing industry to military technology, I trace the conversations regarding computer security from the early 1960s until the 1980s. As computing and the internet gained popularity, the rhetoric of computer security transforms into metaphors, packaging within it the anxieties of the AIDS epidemic and the Cold War. While the expert discourse percolated for about a decade, it took became transformative in the aftermath of the Morris Worm, bringing previously insulated conversations into the public spotlight. The Morris Worm is a public spectacle that institutionalized industry discourse within American laws, courts, and security bureaucracies, shaping the structure and understanding of the internet forever.

---

[6] Bryan Pfaffenberger. "The Social Meaning of the Personal Computer: Or, Why the Personal Computer Revolution Was No Revolution." *Anthropological Quarterly* 61, no. 1 (1988), 1.
[7] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*. New York: ACLS History E-Book Project, 2005, 7.

The Emergence of Computing and the Internet

Early years of the computing developments were intimately tied to the United States military and government apparatuses. The contribution of the scientific community to the Allies' victory during WWII ranges from decryption to the bombing of Dresden, Tokyo, Hiroshima, and Nagasaki. Even despite the self appraised neutrality of the scientific community during the post-war years, their achievements are difficult to separate from the demands of the Cold War security struggles.[8] Even as the internet escaped the direct grasp of government services, the academic researchers continued to articulate security-centric motivations to justify their work. Once the internet entered the public domain, an onslaught of security breaches pushed the United States Congress to construct limits around proper computer behavior, and the computer science community used contagion anxieties of the 1980s to articulate technical intricacies to a lay audience.

Prior to the emergence of the internet computing power was tightly coupled to the American security demands. While technologies operating on autonomous circuitry had existed prior to the 1940s, World War II became the push to accelerate the nascent technology. One of the most cumbersome problems for the Allies concerned airplanes. Flight has evolved significantly since World War I, and very few gunners could accurately handle anti-aircraft artillery.[9] The earliest solutions involved a myriad of math tables that came to be known as a "gun directory," an electromechanical operator able to quickly measure an enemy plane's future position and automatically move itself based on the directory's output. The mathematicians that worked on these problems during the early years of World War II came to be known as

[8] Audra J Wolfe. *Freedoms Laboratory: the Cold War Struggle for the Soul of Science*. Baltimore, MD: Johns Hopkins University Press, 2018, 12.
[9] Edwards, *The Closed World,* 45.

"computers."[10] But the human "computers" made mistakes and the exacerbation of the war required scalability. The Electronic Numerical Integrator and Calculator (ENIAC), was created with a Department of Defense grant to calculate the "gun directory" almost a hundred times faster. Herman Goldstine, the director of the ENIAC pointed out that "the automation of this process was… the raison d'etre for the first electronic digital computer."[11]

The investment that made the ENIAC possible continued to soar even after the war had ended. In an address to President Roosevelt, Vannevar Bush articulated the vision of American military superiority based on scientific progress rather than strategy:

> This war emphasizes three facts of supreme importance to national security: (1) Powerful new tactics of defense and offense are developed around new weapons created by scientific and engineering research; (2) the competitive time element in developing those weapons and tactics may be decisive; (3) war is increasingly total war, in which the armed services must be supplemented by active participation of every element of the civilian population.[12]

The time element became the vital factor in 1949, when the Soviet Union exploded its first atomic bomb.[13] The race against Communism constructed a political dogma based squarely on scientific superiority. Starting with the SAGE air defense system that would "use computers for an entirely new purpose of real-time control and the integration of multiple data sources," American military apparatus harnessed the full might of universities, researchers, and civilians in a desperate attempt to be first.[14] From the 1950s through the 1960s, more than 25 similar military computing systems were designed based on SAGE. Hundreds of university departments and private industries were created to ensure American computing came out ahead.

---

[10] Ibid.
[11] Ibid., 49.
[12] Ibid., 58.
[13] Martin Campbell-Kelly, *The History of the Internet*, 17.
[14] Christos Moschovitis. History of the Internet: a Chronology, 1843 to the Present. Santa Barbara, CA: ABC-CLIO, 1999, 34.

As the Cold War heated up, so did visions of ambitious and far-reaching projects. One week after the Soviet Union successfully launched Sputnik into space, the US government established the Advanced Research Projects Agency, with the "stated mission of keeping the United States ahead of its military rivals by pursuing research projects that promised significant advances in defense related fields."[15] Rising fears of nuclear war created room for previously untenable projects to take shape. In 1964, a RAND Corporation engineer Paul Baran wrote an article contemplating the worst case nuclear scenario, and imagined a communication system with no central authority that "would be designed from the get-go to transcend its own unreliability" and could be used by survivors to communicate safely across the country.[16] The development that distinguished this network from a telephone line centered on how information traveled. Rather than sending information in one piece, via one cable, a message would be broken down, sent in pieces, and reassembled at the endpoint.[17] Baran became one of the earliest scientists to articulate a vision for what a national internet would look like.

ARPA directors and scientists became genuinely interested in the possibility of a secure national network. Despite certain historical accounts, Paul Baran wasn't the first to imagine what a packet switching network would look like.[18] Robust time-sharing projects, that allowed researchers to access large computing systems from the other side of the country were already taking shape at universities across the country. The first successful internet-based logic system, Compatible Time Sharing System, emerged out of the Massachusetts Institute of Technology in 1961.[19] Not wanting to start from scratch, the first ARPA director, JCR Licklider, gave his alma

---

[15] Karl de Leeuw. The History of Information Security: a Comprehensive Handbook. Amsterdam: Elsevier, 2007, 745.
[16] Bruce Sterling. "Science Fiction And The Internet." *Reading Science Fiction*, 2008, 235–43, 239.
[17] Roy Rosenzweig. "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet." *The American Historical Review*, 1998.
[18] Ibid.
[19] Martin Campbell-Kelly, *The History of the Internet*, 24.

mater, MIT, a $3 million grant to continue research into time sharing systems.[20] Universities quickly became hubs of internet researchers, creating lucrative opportunities for researchers to pursue computing projects under the guise of plausible deniability regarding their relations to military interests.

From its active role in WWII research, MIT quickly gained a reputation as the center of computing research. Licklider's replacement at ARPA became Ivan Sutherland, another MIT graduate who happily wrote a $7 million grant to his alma mater for MULTICS, an evolution on timesharing technology that could handle thousands of users simultaneously.[21] The campus also became a cultural hub for computing enthusiasts. The term "hacking" was originally used by MIT to describe physical pranks until the early 1960s, when it permanently slipped into the halls of the computer science department.[22]

The concept of entering a computer system without permission didn't only preoccupy computer science students. As early as 1966, the House of Representatives held a week-long meeting to discuss the potential threat computers may have on privacy.[23] While the meetings were comically unproductive, they attempted to dissect issues that would become central once computing grew in scale, including the potential for adversarial intrusions. In a prescient turn of events, less than two years later, the West German police caught an East German spy snooping through the files of the IBM's German offices in what some have called the first case of computer crime.[24] The spy had tried to physically insert a disk into the computer, but researchers had already started sounding theoretical alarms about the possibility of remote access.

---

[20] Ibid., 23.
[21] Moschovitis. History of the Internet: a Chronology, 79.
[22] De Leeuw, *The History of Information Security,* 752.
[23] U.S. Congress, House of Representatives, Committee on Government Operations, *The Computer and Invasion of Privacy*, 89th Congress, 2nd Session, 1966.
[24] Michael Warner. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. 5 (2012): 781–99, 784.

The conversations surrounding security and privacy proliferated throughout bureaucratic ranks. In October of 1967, the Defense Science Board led a study group to examine the risks of computing. The RAND Corporation published the classified findings in February of 1970, predicting that engineering will not be able to solve the issues of computer security.[25]

> 3. Contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.
> 4. It is unwise to incorporate classified or sensitive information in a system functioning in an open environment unless a significant risk of accidental disclosure can be accepted.[26]

For most of the 1970s, securing systems depended on what Michael Warner termed "hygiene over hardware."[27] Most administrators focused on encryption, privileged access, and hashed passwords.

Simultaneously, concerns about the government's relationship with the nascent computing industry garnered serious attention. When the National Bureau of Standards called for an encryption algorithm to safeguard government information, IBM developed the Digital Encryption Standards (DES) in collaboration with the NSA.[28] The relationship was as successful as it was controversial. Fear over the NSA's role in potentially manipulating a backdoor into the DES prompted an investigation by the Senate. While the committee did not find anything to corroborate the rumors, it became the first investigation into the inevitable tension between the

---

[25] Ibid.
[26] "Report of the Defense Science Board Task Force on Computer Security," Security Controls for Computer Systems, published by RAND for the Office of the Director of Defense Research, 1970 as cited in Michael Warner. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. 5 (2012): 781–99, 784.
[27] Ibid., 785.
[28] Albert Gersho. "Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard." *IEEE Communications Society Magazine* 16, no. 6 (1978): 53–55, 52.

openness of the internet, perceptions of its insecurity, and fears of governmental overreach in the guise of protection.

A government-sponsored internet network created more connections and inevitably, more concerns. The greatest leap for networking came when ARPA decided to connect the timesharing projects it had incubated at MIT, UCLA, Berkeley, and Stanford.[29] While many networking projects were being seriously tackled by private institutions and governments across the world, by 1978 the United States discovered a way to connect all of those disparate systems. Advances in communication protocols allowed ARPA to communicate between systems that were using different algorithms or even if they were running on different infrastructures.[30] The new standards started to slowly introduce computing and the new methods of communication into the mainstream.

The advent of personal computers further democratized the internet beyond the academy's wildest imagination. Through the bulletin board model, Compu-serv and BBS became the first online communities to create communal forums for sharing information about the newly emerging computer world.[31] To give a sense of the internet's popularity, by the summer of 1984, CompuServe had 130,000 subscribers and 26 mainframe computers.[32] While the internet was far from becoming mainstream, the self-selected community of tinkerers and "hackers" had begun experimenting with the limits of permissible online access.

One of the first "unauthorized computer access" cases to confirm the theoretical suspicions of the RAND researchers in 1984. A group of high school students from Milwaukee

[29] Martin Campbell-Kelly, *The History of the Internet*, 25.
[30] Fred Kaplan. *Dark Territory: the Secret History of Cyber War*. New York: Simon & Schuster Paperbacks, 2017, 53.
[31] Warner, *Cybersecurity: A Pre-History,* 787.
[32] Ibid.

referring to themselves by their area code - the 414s - used the Telenet networks to access various computers across the country, including the unclassified military networks at Los Alamos.[33] The case quickly captured the public's attention; a congressional report from 1984 mentioned that the case "was reported in virtually every newspaper and television news program in the country. Interviews were conducted on national television programs, and Johnny Carson included the incidents in his monolog."[34] Since no laws regarding proper computer access had existed prior to this moment, the case was shrouded in genuine confusion. he incident highlighted both the ambiguity of computer-related legal statutes and popular perception of the ethics involved in entering a foreign computer system. When a congressman asked Neal Patrick, the leader of the 414s, when he knew that they stepped out of bounds, Patrick responded: "when the FBI showed up at my door."[35]

The public scrutiny of the case demanded answers. Numerous media outlets pointed blame directly at government administrators. In September of 1983 story on the 414's, the *New York Times* pointed out that the Department of Defense has become "increasingly concerned about their future security," doubting that their 8000 networked computers were, in fact, impregnable.[36] Donald Latham, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence told the *Times* that "there'll be more of these hackers, and we're going to have to deal with their increasing sophistication."[37] But none of the 414 hackers were ever charged or sentenced for their curious exploits.

---

[33] David Bailey. "Attacks on Computers: Congressional Hearings and Pending Legislation," *1984 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1984, 181.
[34] Ibid., 182.
[35] Ibid.
[36] William Broad. "Computer Security Worries Military Experts." *The New York Times*, September 25, 1983.
[37] Ibid.

Legal institutions across the country were slow to catch up to the emergence of computer crime as a serious standard of analysis. From the 1970s to the 1980s, most legal conversations mostly grappled with questions of trespassing. Can information stored within interconnected and accessible networks be considered private property? Is entering someone else's computer from the other side of a country the same as walking into someone's house? How important is intent for effective and just prosecution? For most of the early 80s, computer crime was prosecuted under almost 40 different statutes.[38] Minnesota was the first state to pass a law specifically related to computer crime in 1982, but even they did so by merely extending wire fraud, embezzlement, and theft statutes to a new vocabulary terrain: "computers."[39] Comprehensive federal legislation didn't come about until the 414s made computer crime impossible to ignore.

The Computer Fraud and Abuse Act, passed in 1984, responded to growing pressure to secure federal networks. The virtual breakin by high school students into the Los Alamos National Laboratories, coupled with extensive media scrutiny, and pressure from reports by the American Bar Association pushed Congress to define computer crime as a separate legal category.[40] The law focuses on three narrow issues.

> First, the Act made it a felony to knowingly access a computer without authorization in order to obtain classified United States military or foreign relations information with the intent or reason to believe that such information would be used to the detriment of the United States. Second, the Act made it a misdemeanor to knowingly access a computer without authorization to obtain information protected by federal financial privacy laws. Finally, it created a misdemeanor to knowingly access a federal government computer without authorization and thereby use, modify or destroy information therein, or prevent authorized use of such computer.[41]

---

[38] John Montgomery. *White-Collar Crime: Fourth Survey of Law*. Washington, D.C.: Georgetown University Law Center, 1987, 23. The most common laws used to prosecute computer crime was the theft and federal mail fraud statutes.
[39] Ibid.
[40] *Computer Fraud and Abuse Act of 1986: Report (to Accompany H.R. 4712) (Including Cost Estimate of the Congressional Budget Office)*. Washington, D.C.: U.S. G.P.O., 1986. The Congressional Budget Office estimated that computer crime was causing financial losses between $145 million and $730 million annually.
[41] Susan M. Mello, "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris," Rutgers Computer & Technology Law Journal 19, no. 1 (1993): 259-280, 262.

The act was extremely limited in scope, reflecting much of the popular doubt that computer systems would ever seriously extend outside of academic and government use. Immediate legal criticism also highlighted its lack of a broad definitional reach or use for prosecution.[42] An amendment passed in 1986 raised the criminal standard from "knowingly" to "intentionally," clarified certain definitions, and added three new offenses.[43] But the jurisdiction remained only pertinent to cases related to federal interest.

For the first time, a popular case created room to discuss internet security with genuine federal urgency. The year of the Los Alamos hacks, Ronald Reagan passed the National Security Decision Directive (NSDD) to protect federal information systems. Almost overnight, NSA became responsible for overseeing, researching, and protecting all "government telecommunications systems and automated information systems."[44] While testifying to a House committee, Donald Letham emphasized that "virtually every aspect of Government and private information is readily available to our adversaries" and "unfriendly governments and international terrorist organizations are finding easy pickings."[45] In the eyes of many critics, the federal government used the urgency of the catastrophic vision media outlets constructed out of the 414 incident to grasp greater control of internet networks.

Many in Congress pushed back against what seemed like a clear governmental overreach. Several pieces of legislation were brought up to challenge Reagan in meetings held by the House Government Operations committee between 1985 and 1987. One of the NSA's most ardent

---

[42] Ibid., 257.
[43] Ibid., section (a)(3) was modified as only a trespass consideration. "having accessed a computer with authorization" was replaced with "or exceeds authorized access." Three new offenses included "a felony provision for malicious damage to a federal interest computer, a felony provision for computer fraud, and a misdemeanor offense for trafficking in computer passwords."
[44] Warner, *Cybersecurity: A Pre-History,* 789.
[45] Linda Greenhouse, 'Computer Security Shift is Approved by Senate', New York Times, 24 December 1987. as cited in Warner, *Cybersecurity: A Pre-History,* 788.

critics, Rep. Jack Brooks called the NSDD "an unprecedented and ill-advised expansion of the military's influence in our society."[46] A diverse concoction of interest groups argued that the NSA presents serious dangers to the future of the internet. Lobbyists ranging from "the American Bankers Association to the American Civil Liberties Union urged Congress to limit the Defense Department's powers to cite national security grounds in restricting public access to online information."[47] The 1980s began to outline the boundaries of permissible dialogue about internet access, civil liberties, and the Government's stake in regulation. It wouldn't be the last time internet security went through the incident-panic-response model of regulation.

In the same year that the vision of the RAND scientists came true with the 414s, a computer scientist from USC demonstrated another, palpably worse security scenario of the future. At a security conference at Lehigh University, Fred Cohen, at the time a PhD student at USC, demonstrated how a code inserted into a computer system connected to the internet can easily spread to everyone connected on the network.[48] Two years later, in his PhD dissertation, Cohen coined the term "virus" or "a program that can 'infect' other programs by modifying them to include a possibly evolved version of itself."[49] He expands on the process by pointing out "with the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows."[50] The term virus didn't gain in popularity until its "existence in the wild" would be confirmed three years later.

---

[46] Ibid.
[47] Ibid.
[48] Fred Cohen. "Computer Viruses: Theory and Experiments." *Computer & Security* 6 (1987): 22–35, 23.
[49] Ibid., 24.
[50] Ibid.

A student armed with a computer, curiosity, and access to Cornell's computer system would confirm Cohen's fears and create a new problem for legislators and bureaucrats alike. The history of computer crime cannot be told either as a uniform manifestation of bureaucratic whims nor a technological wild west. The way security official and the American public perceived the internet and its security were colored by the militarized history of the internet, anxieties of the 20th century, and administrative tug-o-war for control of a growing industry. This section provided the context for the proliferation of internet crime, legislative responses, and popular perceptions just before the internet as we know it would take over the world. By looking closely at the Morris Worm in the next section, this paper will highlight how conversations regarding poorly understood technology rely on metaphors of contagions, as well as how this discourse impacts institutions.

The Target and The Source

When the Morris Worm struck in early November of 1988, the computer science community was genuinely perplexed. By the end of the decade, questions of computer insecurity had started to seriously proliferate throughout research circles. A popular film, a few headline-grabbing computer attacks, and a myriad of legislation concerning computer security defined the early years of the 1980s. But the Morris Worm was different because of its target; it went after the institutions that created the internet. Within three days of its launch, the Worm disabled more than 6,000 government and university computers.[51] While previous cases relied on accessing a computer system physically, Morris' code replicated autonomously and moved

[51] Larry Boettger. "The Morris Worm: How It Affected Computer Security and Lessons Learned by It." Global Information Assurance Certification Paper, December 20, 2000.

through the communication channels usually reserved for official business unnoticed. The meeting organized by the National Computer Security Center in response to Morris brought the foremost experts on computer security together, to discuss American internet concerns, and deal with the Worm's public spillover. The experts in the meeting cemented the discourse of computer crime. While Morris did not single-handedly create the securitized internet familiar to us now, he brought it to the forefront, becoming a conduit through which previously inaccessible conversations could take the public stage.

The self-propagating virus was the first of its time to take on a life of its own after creation. Unlike previous intrusions that had to penetrate the hardware of a computer, the Morris Worm spread seemingly on its own accord. The code targeted three applications, and while it did not explicitly harm operations like access information or delete files, it ended up consuming so much of a computer's resources that it prevented it from carrying out any other function.[52] Within a matter of fifteen hours, over six thousand computers - about 10% of all computers connected in the United States, including those at Wright-Patterson Air Force Base, the Army Ballistic Research Lab, and several NASA facilities - were shut down.[53] While Morris and came up with an antidote to the code, they couldn't distribute it to the network because all of the communication channels were shut down.[54] It took three days for the Worm to be neutralized and operation of ARPANET to return to normal.

The author of the code, Robert T. Morris Jr, was a graduate student at Cornell when he released his creation into the wild. In an interesting turn of events - and one that would fuel

---

[52] Ibid., 15.
[53] National Computer Security Center, "Proceedings of the Virus Post-Mortem Meeting: ARPA/MILNET Computer Virus Attack," November 8, 1988, The National Security Archive, Washington, D.C.
[54] Katie Hafner and John Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York, NY: Simon & Schuster, 1995, 245.

endless conspiracy theories - the creator turned out to be the son of Robert Morris Sr., a chief scientist of the NSA Computer Security Center and the architect of the UNIX system.[55] An internal investigation at Cornell University determined Morris' actions to be "a juvenile act that... may simply have been the unfocused intellectual meandering of a hacker completely absorbed with his creation and unharnessed by considerations of explicit purpose or potential effect."[56] Due to the nature of the code, it was unclear how much Morris should be chastised or thanked. In a presentation regarding the attack, Clifford Stoll, a scientist at Harvard who engineered a solution saved his last slide to pontificate "Did this guy do us a favor by showing our vulnerabilities? Was it necessary? A month ago, cover of time [sic] magazine was about viruses!"[57]

Like the experts, historians have covered Morris' Intention with notable contradiction. While some have chosen to focus extensively on the accidental nature of the code[58], others have squarely placed blame on the author for not properly anticipating its effects.[59] A few historians have attempted to spin the graduate student as a benevolent explorer, who has been forced to take computer security of the country into his own hands after managers of the UNIX software refused to fix several vulnerabilities he had pointed out to them.[60] One writer even painted Morris as an attention seeker trying "to get away from his father's image and have one of his

---

[55] Fred M. Kaplan. *Dark Territory: the Secret History of Cyber War*. New York: Simon & Schuster Paperbacks, 2017, 60.
[56] Eisenberg, *The Cornell Commission*, 1.
[57]Cliff Stoll. "Site Experience: Harvard," *The Morris Worm, 1988,* ed.Michael Martelle, Washington D.C.: The National Security Archive.
[58] Josephine Wolff. *You'll See This Message When It Is Too Late: the Legal and Economic Aftermath of Cybersecurity Breaches*. Cambridge: MIT Press, 2018. and Christos Moschovitis. *History of the Internet: a Chronology, 1843 to the Present*. Santa Barbara, CA: ABC-CLIO, 1999.
[59] Ted Eisenberg, Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, and T. Santoro. "The Cornell Commission: on Morris and the Worm." Communications of the ACM 32, no. 6 (January 1989) and Karl Leeuw. The History of Information Security: a Comprehensive Handbook. Amsterdam: Elsevier, 2007.
[60] Moschovitis. *History of the Internet,* 78.

own."[61] Regardless of his genuine motivation, the divergent narratives of why Morris wrote the code say more about an author's imagination of proper internet behavior than the perpetrator themselves. Self projections and imaginations of the internet's nature shine in the discussions of the affected scientists.

The Post-Mortem and Contagion Discourse

In response to Morris, seven days after the attacks, the federal government organized an impromptu conference with affected parties to understand the consequences of the internet's security vulnerabilities. Coordinated by the National Computer Security Center, the meeting included members of security, internet operation, and academic institutions.[62] Representatives from the Air Force, Army, DARPA, DCA, ASD, DOE, NSA, FBI, NIST, NSCS, and academics from Harvard, Berkey, MIT, and Stanford each brought their unique perspective, imagination, and interest to the meeting.[63] The way these experts discuss the internet, computer viruses, and their personal role elucidate how biological language is imprinted onto technical systems. Their language paints the internet as a living, breathing body, while they become the doctors ready to heal. The authority of natural science permits security experts to imbue their work with certain social significance, while allowing computers, the internet, and the nation "to be articulated in the idiom of organic nature, an idiom that an often obscure the historical and cultural specificity of such conceptions."[64]

---

[61] Larry Boettger. "The Morris Worm: How It Affected Computer Security and Lessons Learned by It." Global Information Assurance Certification Paper, December 20, 2000.
[62] National Computer Security Center, "Proceedings of the Virus Post-Mortem Meeting: ARPA/MILNET Computer Virus Attack," November 8, 1988, The National Security Archive, Washington, D.C, 7.
[63] Ibid.
[64] Stefan Helmreich. "Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism." *Science, Technology, & Human Values* 25, no. 4 (2000): 472–91, 474.

From the start of the meeting, computers are regarded almost exclusively as biological entities. William Sherlin, on behalf of the Defense Advanced Research Project Agency, outlines subheadings in his presentation that might as well be from a medical textbook:

1. THE VIRUS
1.2. SYMPTOMS AND BEHAVIOR
1.3. METHOD OF ATTACK
1.4. ESTABLISHING THE INFECTION
1.5. DETECTION AND DIAGNOSIS
1.6. IMMUNIZATION AND PREVENTION
1.7. ASSESSMENT AND RECOVERY [65]

The DARPA team fully embraced the idea of a living virus. They extend the metaphor, pointing out "the principal symptom of the virus… are degradation of system responses."[66] The computer code itself, removed from the author, becomes endowed with agency to the point where "the principal activity of the virus is to replicate itself and spread to other machines… with resultant degradation of performance."[67] Michael Muuss of the US Army Ballistic Research Laboratory goes a step further to define a virus: "From Latin: slimy liquid, poison, stench… Complex molecules, capable of growth and multiplication only in living cells."[68] The viral contagion becomes seemingly imminent, it lacks a subject or a source, holding within itself only a goal of destruction.

In a world where the goal of computer code is "infection," the defenders become first responders ready to administer the antidote. The DARPA researchers assure listeners that "immunization and/or prevention measures were developed."[69] Michael Muuss, of the US Army

---

[65] William Scherlis and Stephen Squires, "Memorandum for the Director," *The Morris Worm, 1988,* ed. Michael Martelle, Washington D.C.: The National Security Archive, 8.
[66] Ibid, 9.
[67] Ibid.
[68] Michael Muuss, "Site Experience: Army Ballistic Research Lab," *The Morris Worm, 1988,* ed. Michael Martelle, Washington D.C.: The National Security Archive, 5
[69] Sherlis, *Memorandum for the Director*, 9.

Ballistic Research Laboratory, nicknames his scientists the "antiviral team" and the management "virus busters."[70] In almost every sense, the danger of the virus to the communal immunity can only be thwarted by experts with the tools who understand the body.

The Ballistic Corp simultaneously demonstrated concern regarding the public perception. An aura of public spectacle hangs over most of the presentations. In the final report about the meeting, NSCS highlights a need for "a single USG focal point at the national level to interact with the press."[71] While the final editors emphasized the need for efficiency and coordinated messaging, some presenters expressed concern over a possible panic. Anticipating that his biological metaphors might be too successful, Muss wrote "My fear: these headlines: 'Computer Virus Spreads to Humans: 96 left dead…[sic]."[72]

The construction of a vulnerable body-internet is significant for the solutions that the metaphors demand. Contagion metaphors on the internet are intimately tied to the bodily anxieties of the 20th century. When the rise of virology as a field coincided with the McCarthy trials, "viruses increasingly assumed the characteristics of communists; they were devious and sinister, forming a kind of fifth column."[73] The viral model of a healthy body fighting off an infection is imbued with a number of assumptions about sovereignty, foreignness, and immunology. The viral contagion demands an "enormous quantities of centrally, if not globally, managed funds and research as well as the institutionalization of global biopolitical strategies of surveillance, diagnosis, containment, eradication, and therapy."[74] A backbone of vigilance is installed, turning every internet user into a potential organism that is a bundled potential of viral

---

[70] Muuss, *Site Experience*, 8.
[71] National Computer Security Center, *Proceedings of the Virus Post-Mortem,* 89.
[72] Muuss, *Site Experience*, 17.
[73] Zahi Zalloua and Bruce A. Magnusson. *Contagion: Health, Fear, Sovereignty*. Seattle and London: University of Washington Press, 2012, 43.
[74] Ibid., 6.

energy.[75] The NCSC experts are inadvertently mobilizing fear and anxiety, aware that it must contaminate other discourse if it is to be successful.

Judicial, Legislative, and Bureaucratic Spillover

The discussions of computer viruses, the internet, and viral immunity extended far beyond the insular confines of the NCSC meetings. Experts present at the meetings provided legal advice, advised members of congress, and went on to head leading cybersecurity firms. The rhetoric of contagion and immunal metaphors had broad-reaching impact on court precedents, on internet legislation across the country, and on the ways American citizens interacted with their computers. The following section traces the discursive spillover into the popular consciousness. The Morris incident became the vehicle to bring private conversations that computer experts had been having regarding perceived internet vulnerability into the public. It was this spillover that would have the most lasting effect on legislation, legal precedents, and an emerging computer security industry.

Judicial Discourse

Three years after it was passed, Robert Morris became the first person to be prosecuted under the 1986 Computer Fraud and Abuse Act. The Northern District of New York indicted Morris on misdemeanor and felony provisions of the Act, covering

> [I]ntentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby

[75] Stefan Elbe. "Bodies as Battlefields: Toward the Medicalization of Insecurity." *International Political Sociology* 6, no. 3 (2012): 320–332, 323

> (A) causes loss to one or more others of a value agregating $1,000 or more during any one year period.[76]

Morris' defense disputed, arguing that under the law "he not only had to intentionally access a federal interest computer, but he also had to intend to prevent authorized use of those computers."[77] The cases rested on the argument that Morris did not exceed his authorized access as a student with full access to the computer networks of Cornell University, and did not intend to cause damage since he attempted to release a fix. After the district judge ruled that no legislative history is required because the CFAA seemed "unambiguous," he ruled against Morris, deciding that intent "requirement did not apply to the damage clause."[78] The appellate court disagreed with the district's decision regarding the Act's "unambiguous" clarity, reviewing the case upon the vagueness of the punctuation, and whether "intentionally" only modified the "access," or included the "damage" clause. Upon review of the legislative history, they concurred with the district court, concluding that only intent to access is necessary to prosecute under the Computer Fraud and Abuse Act.

The prosecution of Morris became pivotal for future computer crime cases. While the Supreme Court refused to hear the case without comment, the appellate decision set two important legal precedents. First, they established the minimum prosecutorial requirement for the Act to be intentional access, rather than intentional damages. Second, they cemented the definition of an "outsider" as anyone who uses a computer program or accesses a computer

---

[76]Camille Marion, "Computer Viruses and the Law," Dickinson Law Review 93, no. 3 (Spring 1989): 625-642, 630.
[77] Susan M. Mello, "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris," Rutgers Computer & Technology Law Journal 19, no. 1 (1993): 259-280, 263.
[78] Ibid., 268.

network without authorization, creating a bubble of legal sovereignty around each individual computer system and program.[79] Judge Jon Newman ruled:

> Morris did not use either of those features [the email and directory applications] in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.[80]

The issue wasn't that Morris didn't get permission to tinker with the programs from the University, but rather that the designers of the exploited programs did not intend users to interact with their applications in the way he did.

The sentencing of the case also charted new territory. While the prosecution attempted to impose a twenty seven month prison sentence, the defense vied for six. The judge expressed the difficulty of finding a precedent for sentencing such a new crime, saying "the dollar loss overstates the seriousness of the offense."[81] Many critics expressed dismay in private, one saying "if a person hasn't acted with malicious intent, it's not quite clear what you're trying to deter."[82] At the end of the trial, the judge concluded that in order to prevent future "hackers" from attempting to access unauthorized domains, Morris was sentenced to three years probation, 400 hours of community service, and a fine of $10,050.[83] The case highlighted the difficulty of prosecuting such a new realm, applying legal concepts to an undefined and misunderstood domain, as well as the limits and ambiguities of the 1986 Computer Fraud and Abuse Act.

---

[79] Ibid., 271.
[80] Josephine Wolff. *You'll See This Message When It Is Too Late: the Legal and Economic Aftermath of Cybersecurity Breaches*. Cambridge: MIT Press, 2018, 213.
[81] Mello, *Administering the Antidote*, 275.
[82] Marc Rotenberg, Office Director of Computer Professionals for Social Responsibility, *quoted in* Susan M. Mello, "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris," Rutgers Computer & Technology Law Journal 19, no. 1 (1993): 259-280.
[83] Ibid., 275.

The incident brought conversations about computer viruses to congress. Like the 414s that inspired the 1986 legislation, Morris would usher into Congress a new era of computer virus discourse. After the attacks gained national attention, the Senate Judiciary Committee established a subcommittee on Technology and the Law, which started holding hearings on "Computer Viruses" in May of 1989.[84] During the testimony of the first panel, William Sessions, the Director of the Federal Bureau of Investigation, opened by highlighting the limitations of the Computer Fraud and Abuse Act and first uttered the word "virus" on record.

> In the context of our investigative responsibilities, we have found that existing federal statutes are generally adequate when the computer-related criminal acts parallel common law crimes such as embezzlement, fraud, thefit, and destruction of property… Existing criminal statues [sic] however, are not specific on the question of whether unauthorized access is a crime where no theft or damage occurs, and there is no statute specifically addressing viruses. Current criminal statutes, by and large, address the issue of computers as the vehicle of the crime… we have seen an increase in crimes in which the computer or computerized information is the target of the crime. Computer viruses present one such example… With today's technology, viruses can begin the infectious process from a home personal computer, an office, an academic institution, or from almost anywhere in the world.[85]

Sessions addressed all the issues highlighted throughout Morris' court proceedings, urging Congress to pass legislation that would target viruses directly.[86] During the second panel testimony, Clifford Stoll, who wrote the code that stopped the Morris Worm at Harvard, spoke of the virus incident without ever mentioning it by name. At the end of his testimony, he reiterated the hypothetical question he posed to the NCSC related to Morris' guilt: "Or might this virus be a useful way to raise our consciousness of computer security? A quaint attempt to tell us to

---

[84] U.S. Congress, Senate, Judiciary Subcommittee on Technology and Law, *Hearings on Computer Viruses,* 101 Congress, 1st session, May 15, 1989.
[85] U.S. Congress, Senate, Judiciary Subcommittee on Technology and Law, *Hearings on Computer Viruses,* 101 Congress, 1st session, May 15, 1989 (opening testimony of William Sessions).
[86] Ibid.

secure our computers? We don't thank burglars for reminding us that our houses are insecure… There are more ethical ways to spread the word."[87]

The court case and congressional meetings would usher in a new era of computer crime legislation. Morris highlighted the inadequacies of the computer laws that were drafted without considerations that internet technology would ever spread outside of military and scientific circles. The conversations around computer insecurity that had gained traction within specialist circles as early as 1966 found an official outlet through the attention-grabbing mistake of Robert Morris. The security imagination, rhetorical metaphors, and institutional demands of computer scientists and investigative bureaus played a major role in the securitization of computer networks.

Legislative Discourse

Legislation introduced at the end of the 1980s directly referenced the legal challenges surrounding viruses and Morris. Subsequent federal bills attempted to extend the scope of older statutes. Representative Wally Herger introduced the Computer Virus Eradication Act (CVEA) of 1989 to amend the CFAA with the section:

> Whoever knowingly inserts into a program for a computer, or a computer itself, information or commands, knowing or having reason to believe that such information or commands may cause loss, expense, or risk to health or welfare -
>
> (i) to users of such computer or a computer on which such program is run, or to persons who rely on information processed on such computer; or
>
> (ii) to users of any other computer or to persons who rely on information processed on any other computer; and provides (with knowledge of the existence of such information or commands) such program or such computer to a person in circumstances in which such person does not know of the insertion or its effects; if inserting or providing such information or commands affects, or is affected or

[87] U.S. Congress, Senate, Judiciary Subcommittee on Technology and Law, *Hearings on Computer Viruses,* 101 Congress, 1st session, May 15, 1989 (written statement of Clifford Stoll).

> furthered by means of, interstate or foreign commerce [shall be punished as described].[88]

The bill attempted to expand beyond just federal computer networks, putting private firms within its purview. To elucidate technical aspects of computerized systems and extend understanding to the private domains, legislators often borrowed the medicalized rhetoric of computer scientists. Compelling cases centered on drawing direct connections between the urgency of the internet security and the contagion outbreaks of the decade. In her statements on the necessity of the CVEA, Herger made an explicit link to HIV, saying "Some have called [a virus] the AIDS of the computer world."[89] Such discourse quickly trickled down to the local level.

State legislatures across the country began to explicitly and expeditiously legislate computer crime. Prior to 1989, no state had directly mentioned a computer "virus" and a few had the means to even attempt to prosecute it; two years later, Pennsylvania, Maryland, Texas, California, Illinois, and West Virginia enacted laws making the release of computer virus a crime.[90] Minnesota, a state with one of the earliest statutes on computer crime, enacted the Computer Virus Act in August of 1989, explicitly defining a destructive program.

> A computer program that performs a destructive function or produces a destructive product. A program performs a destructive function if it degrades performance of the affected computer, associated peripherals or a computer program; disables the computer, associated peripherals or a computer program; or destroys or alters computer programs or data.[91]

---

[88] H.R. 55, 101st Cong., 1st Sess. (1989). As quoted in Daniel J. Kluth, "The Computer, Virus Threat: A Survey of Current Criminal Statutes," Hamline Law Review 13, no. 2 (Spring 1990): 297-312.
[89] Helmreich, *Flexible Infections*, 486.
[90] Kluth, *The Computer, Virus Threa*t, 308.
[91] Ibid., 310.

The debates of the definition relied heavily on legal and scientific testimonies heard throughout Congress that year.[92] More explicitly, the law's language is almost indistinguishable from the definitions of a virus provided by experts during the NSCS meeting. It's difficult not to see similarities between Minnesota's law and William Sherlin's testimony on behalf of DARPA: "the principal activity of the virus is to replicate itself and spread to other machines… with resultant degradation of performance."[93] In the 1990's, the medicalized rhetoric of computer technicians began to be directly inscribed into the legal code of the United States, giving popular anxieties and contagion metaphors tangible, and institutional expression.

At the helm of the Morris Worm, computer crime started to peak international attention. In 1989, the Council of Europe published a report urging countries to create a unified set of principles that to ensure efficient response to cybercrime.[94] As more countries began to seriously adopt internet protocols, a push for legal standardization accelerated. In 1990, the United Nations' Congress on the Prevention of Crime and the Treatment of Offenders called on countries to "combat cybercrime by modernizing their law, improving computer security and promoting a comprehensive international framework of standards for preventing, prosecuting, and punishing computer related crime."[95]

Bureaucratic Intervention

The expansion of legal coverage into private domains coincided with the birth of a computer security industry. In the process of the medicalization of computer security, academics

---

[92] Ibid.
[93] Muuss, *Site Experience*, 8.
[94] Susan Brenner. "History of Computer Crime." In *The History of Information Security*, 1st ed., 705–21. Elsevier Science, 2007, 715.
[95] Ibid.

and security officials suggested a security-umbrella approach to protecting national networks. When the virus was constructed as a body without organs, a top-down panic created a need for an orchestrated and efficient response. The recommendations from the NCSC post-mortem meeting outlined the strokes of an institution to coordinate the security of the nationalized internet. The meeting gave birth to two structures that continue to impact the direction of computer security: the Computer Emergency Response Team and commercialization of computer security.

The NCSC meeting identified the decentralized network of computer scientists that helped thwart the Worm. Those invited to the meeting were the wounded parties, but also the source of the virus' solution. The academics from Harvard, Berkeley, MIT, Stanford, and auxiliary institutions were termed the "old boy network": partly representative of the computer science demographics, and partly reflecting the relationship of government agencies with academic research circle.[96] The fourth recommendation outlined the need to centralize and maintain the "technical relationships with the computer science 'old boy network'," emphasizing that their "consensus, support, and trust is required" for government security offices.[97] The parties represented at the meeting, from the broad range of universities to the military research institutions, became the vanguard for securing American networks. The connections have often blurred the lines between the self-perception of scientists as purely independent actors.[98]

The coordination between researchers and the military was quickly institutionalized. The NCSC was intentional in emphasizing the need for more than an informal network of computer

[96] National Computer Security Center, "Proceedings of the Virus Post-Mortem Meeting: ARPA/MILNET Computer Virus Attack," November 8, 1988, The National Security Archive, Washington, D.C, 95.
[97] Ibid.
[98] Wolfe. *Freedoms Laboratory,* 13.

security. The first recommendation emphasized the need for an establishment of a "centralized coordination center" managed by the NSA and NIST, serving as a "place to report problems and request solutions," with potential to evolve into a "national-level command center supporting the government and private sector alike."[99] A month later, DARPA established the Computer Emergency Response Team (CERT) at Carnegie-Mellon University to coordinate nationwide network security. Beyond just being a repository of security experts, the organization became responsible for "reporting incidents, conducting security research, and educating the computer user community about security issues."[100] Funded by the Department of Defense, CERT focused exclusively on ARPANET and Milnet, reiterating the government's focus on federally valuable networks. Prior to the birth of a popularly accessible internet, DARPA predicted the need for a more expansive security apparatus, announcing in their press-release "each major computer community may decide to establish its own CERT."[101] That's exactly what happened.

The birth of the World Wide Web created a private computer security industry. During the early 1990s when the internet was starting to take shape as a popular application, the emergence of corporate connectivity online raised immediate vulnerability concerns. Commercial anti-virus and computer security systems first became available to enforce rules about who may access certain resources existing on a network: focusing on password security and the source of internet traffic.[102] Many of these early firms emphasized their ability to keep a private network isolated from outside intrusions, referring to their systems as "firewalls."[103]

---

[99] National Computer Security Center, "Proceedings of the Virus Post-Mortem Meeting: ARPA/MILNET Computer Virus Attack," November 8, 1988, The National Security Archive, Washington, D.C, 95.
[100] Laura DeNardis. "A History of Internet Security." In *The History of Information Security*, 1st ed., 681–704. Elsevier Science, 2007, 685.
[101] Ibid., 686.
[102] Myriam Dunn Cavelty. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge, 2009, 174.
[103] Eugene Schultz. "Internet Security: Risk Analysis, Strategies, and Firewalls." *Network Security* 1997, no. 7 (1997), 15.

Usually regarded as a marketing ploy used to emphasize the conceptual parallels between physical damage and cyber intrusions, firewalls became technical arbiters of who belonged on a network and who was considered a "foreigner."[104]

Private firms continued to capitalize on accepted computer security metaphors to make the technical aspects palatable to corporate buyers. Danny Hillis, an early computer security entrepreneur and a 1988 graduate of the MIT computer science department, emphasized the need of biological metaphors after the Morris incident:

> So long as formats like UNIX become a universal standard, we'll have awful problems with viruses no matter how many vaccines and quarantines we come up with. What we want in networked computing is a diversity of operating standards. We want each computer to be a slight variant of the standard, maybe one that is slowly evolving.[105]

Computer security industry focused on making their software a medical necessity by highlighting their similarity to contagion risks from biological epidemics. One of the largest firewall firms of the 1990s wrote in a promotional research booklet that "like the human AIDS virus that mutates frequently to escape detection by the body's defenses, the polymorphic computer virus likewise mutates to escape detection by anti-virus software that compares it to an inventory of known viruses."[106] The parallels of HIV imagery and computer viruses quickly spilled over into the marketing firewall systems in terms of prophylactic software, like Virusafe, Flu Shot +, Vaccinate, and Disk Defender.[107]

---

[104] Ibid.
[105] Helmreich, *Flexible Infections*, 486.
[106] Symantec. 1999. Computer viruses: An executive brief. Cited in Helmreich, *Flexible Infections*, 487.
[107] Andrew Ross. 1991. "Hacking away at the counterculture." In *Technoculture*, edited by Constance Penley and Andrew Ross, 107-34. Minneapolis: University of Minnesota Press, 124.

Conclusion

The Morris Worm became the event to catapult insulated contagion rhetoric to the public. Through legal and industry channels, metaphors of the body, immunity, and medicalization became institutionalized. The laws passed after the Morris incident defined the internet before it gained serious popularity in the 1990s. And the redefined private industry and security relationships to the internet continue to influence private interactions with computerized networks. Robert Morris wasn't the cause for the evolution. As early as the 1960s, internet researchers were aware of the infrastructure's vulnerability. But it was the particular popularity of the incident that formed the umbrella of institutional anxiety.

It is vital to acknowledge the contingent elements Morris created. The ways in which CFAA was enforced by placing security responsibility on the users rather than program designers is both responsible for the rapid, unabated growth of the internet and simultaneously its tendency to scapegoat actors outside of the computer officialdom. The narrative of internet security is as rhetorically constructed as it is technically mediated. Insecure by design, the internet vanguard has laid the "infrastructure of surveillance, vigilance, and counter-epidemic action," making anxiety the driving force of the internet's globalization.[108] But even as the internet exists in a permanent state of emergency, immunity is perpetually latent. To defend the internet from foreign bodies encroaching on its freedom, the internet itself must be quarantined, protected, and surveilled. Jacques Derrida aptly notes that in the process of immunity, "a living being, in a quasi-suicidal fashion, 'itself works to destroy its own protection, to immunize itself

[108] Zalloua, *Contagion: Health, Fear, Sovereignty*, 6.

against its 'own' immunity."[109] In an ironic fashion, it is most often the metaphors used to liberate technology that binds it the most.[110]

The constraints of American technological industries don't end at the border. Important dilemmas lie in understanding how domestic rhetoric promulgates outside of national boundaries. As early as 1996, Russian and Chinese leaders have reiterated concerns about the connection between American security agencies and privately exported infrastructure. In a 1996 *Pravda* interview, a general at the Chamber of Trade and Commerce said:

> Many people are happy that they got access to the Internet Web, but the owners are American, not us. Now in Russia lots of American servers have been set up, and they supply their equipment for low prices… We must remember about the 'logical bombs' inlaid in their programs. Can you imagine what would happen if one day on a special command all the equipment will be paralyzed.[111]

Similar worries were raised in a 1996 article in the *Liberation Army Daily,* that pointed out the concerns with new communication networks, saying "an information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from its enemy."[112] Chinese and Russian officials express the same concerns that the US Congress, academics, and security officials have voiced since the 1970s. An investigation into the potential spillover of security rhetoric and ideological exportation could reap useful insights into the impact of nascent technological discourse on global political exchanges.

---

[109] Giovanna Borradori. *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Jacques Derrida*. Chicago: Univ. of Chicago Press, 2009, 94.
[110] Colleen Bell. "War and the Allegory of Medical Intervention: Why Metaphors Matter." *International Political Sociology* 6, no. 3 (2012): 325–28. and Mariarosaria Taddeo. "On the Risks of Relying on Analogies to Understand Cyber Conflicts." *Minds and Machines* 26, no. 4 (2016): 317–21. Both offer useful insight into the effects of language on defining the boundaries of user interaction.
[111] Warner, *Cybersecurity: A Pre-History,* 791.
[112] Ibid.

The discourse of nascent technology shapes the boundaries of permissible user relationships. The fact that the scope of legal and executive reaction to large scale computer threats have not changed since Morris should be a signal of the national imaginative morass.[113] Exacerbating encroachment on personal information and commercialization of surveillance poses threats to the growth of the internet, as well as the narrative of its liberalizing potential. As the Morris Worm demonstrated, every future attack is potential for federal aberration from legal norms, civil rights, and due process. At the end of his Senate testimony, Clifford Stoll shed light on the important dilemma internet regulators have inherited from Morris: "Yet how should we react? One response is to slam doors, and build barriers against outsiders. This will make it tougher for the virus-writers. It'll also make life difficult for those who need to exchange information."[114]

[113] Joshua Hill and Nancy Marion, "Presidential Rhetoric on Cybercrime: links to terrorism?," *Criminal Justice Studies*, 29:2 (2016), 163-177. Larry Boettger. "The Morris Worm: How It Affected Computer Security and Lessons Learned by It." *Global Information Assurance*, December 20, 2000. and U.S. Library of Congress, Congressional Research Service, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John Rollins and Anna Henning, 2009. All have tracked the lack of progress or innovation on national cybersecurity policy.

[114] U.S. Congress, Senate, Judiciary Subcommittee on Technology and Law, *Hearings on Computer Viruses,* 101 Congress, 1st session, May 15, 1989 (written statement of Clifford Stoll).

Bibliography

Primary Sources

Bailey, David. "Attacks on Computers: Congressional Hearings and Pending Legislation," *1984 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1984.

Broad, William. “Computer Security Worries Military Experts.” *New York Times*, September 25, 1983.

Cohen, Fred. “Computer Viruses: Theory and Experiments .” *Computer & Security* 6 (1987): 22–35.

Computer Fraud and Abuse Act of 1986: Report (to Accompany H.R. 4712) (Including Cost Estimate of the Congressional Budget Office). Washington, D.C.: U.S. G.P.O., 1986.

Eisenberg, T., D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, and T. Santoro. “The Cornell Commission: on Morris and the Worm.” *Communications of the ACM* 32, no. 6 (January 1989): 706–9.

Muuss, Michael. "Site Experience: Army Ballistic Research Lab," *The Morris Worm, 1988,* ed. Michael Martelle, Washington D.C.: The National Security Archive.

National Computer Security Center, "Proceedings of the Virus Post-Mortem Meeting: ARPA/MILNET Computer Virus Attack," November 8, 1988, The National Security Archive, Washington, D.C.

Scherlis, William and Stephen Squires, "Memorandum for the Director," *The Morris Worm, 1988,* ed.Michael Martelle, Washington D.C.: The National Security Archive.

Stoll, Clifford. "Site Experience: Harvard," *The Morris Worm, 1988,* ed.Michael Martelle, Washington D.C.: The National Security Archive

U.S. Congress, House of Representatives, Committee on Government Operations, *The Computer and Invasion of Privacy*, 89th Congress, 2nd Session, 1966.

U.S. Congress, Senate, Judiciary Subcommittee on Technology and Law, *Hearings on Computer Viruses,* 101 Congress, 1st session, May 15, 1989 (written statement of Clifford Stoll).

U.S. Congress, Senate, Judiciary Subcommittee on Technology and Law, *Hearings on Computer Viruses,* 101 Congress, 1st session, May 15, 1989 (opening testimony of William Sessions).

U.S. Library of Congress, Congressional Research Service, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John Rollins and Anna Henning, 2009.

Secondary Sources

Bell, Colleen. “War and the Allegory of Medical Intervention: Why Metaphors Matter.” *International Political Sociology* 6, no. 3 (2012): 325–28.

Brenner, Susan. “History of Computer Crime.” *The History of Information Security*, 1st ed., Elsevier Science, 2007, pp. 705–721.

Boettger, Larry. “The Morris Worm: How It Affected Computer Security and Lessons Learned by It.” Global Information Assurance Certification Paper, December 20, 2000.

Borradori, Giovanna. *Philosophy in a Time of Terror: Dialogues with Jürgen Habermas and Jacques Derrida*. Univ. of Chicago Press, 2009.

Broad, William. “Computer Security Worries Military Experts.” *New York Times*, 25 Sept. 1983.

Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge, 2009.

Campbell-Kelly, Martin, and Daniel D. Garcia-Swartz. “The History of the Internet: The Missing Narratives.” *SSRN Electronic Journal*, 2005.

Cohen, Fred. “Computer Viruses: Theory and Experiments .” *Computer & Security* , vol. 6, 1987, pp. 22–35.

Computer Fraud and Abuse Act of 1986: Report (to Accompany H.R. 4712) (Including Cost Estimate of the Congressional Budget Office). U.S. G.P.O., 1986.

Edwards, Paul N. *The Closed World: Computers and the Politics of Discourse in Cold War America*. New York: ACLS History E-Book Project, 2005.

Elbe, Stefan. “Bodies as Battlefields: Toward the Medicalization of Insecurity.” *International Political Sociology* 6, no. 3 (2012): 320–22.

Eisenberg, T., D. Gries, J. Hartmanis, D. Holcomb, M. S. Lynn, and T. Santoro. “The Cornell Commission: on Morris and the Worm.” *Communications of the ACM* 32, no. 6 (January 1989): 706–9.

Gallagher, Cornelius E. “The Computer and the Invasion of Privacy.” *Proceedings of the Fifth SIGCPR Conference on Computer Personnel Research* , 1967.

Gersho, A. “Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard.” *IEEE Communications Society Magazine*, vol. 16, no. 6, 1978, pp. 53–55.

Hafner, Katie, and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon & Schuster, 1995.

Helmreich, Stefan. “Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism.” *Science, Technology, & Human Values* 25, no. 4 (2000): 472–91.

Hill, Joshua and Nancy Marion, “Presidential Rhetoric on Cybercrime: links to terrorism?,” *Criminal Justice Studies*, 29:2 (2016), 163-177.

Kaplan, Fred M. *Dark Territory: the Secret History of Cyber War*. New York: Simon & Schuster Paperbacks, 2017.

Kluth, Daniel. "The Computer, Virus Threat: A Survey of Current Criminal Statutes," Hamline Law Review 13, no. 2 (Spring 1990): 297-312.

Leeuw, Karl de. *The History of Information Security: a Comprehensive Handbook*. Amsterdam: Elsevier, 2007.

DeNardis, Laura. "A History of Internet Security." In *The History of Information Security*, 1st ed., 681–704. Elsevier Science, 2007.

Brenner, Susan. "History of Computer Crime." In *The History of Information Security*, 1st ed., 705–21. Elsevier Science, 2007.

Marion, Camille. "Computer Viruses and the Law," Dickinson Law Review 93, no. 3 (Spring 1989): 625-642

Mello, Susan. "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris," Rutgers Computer & Technology Law Journal 19, no. 1 (1993): 259-280

Montgomery, John. *White-Collar Crime: Fourth Survey of Law*. Georgetown University Law Center, 1987.

Moschovitis, Christos J. P. *History of the Internet: a Chronology, 1843 to the Present*. Santa Barbara, CA: ABC-CLIO, 1999.

Pfaffenberger, Bryan. "The Social Meaning of the Personal Computer: Or, Why the Personal Computer Revolution Was No Revolution." *Anthropological Quarterly* 61, no. 1 (1988).

Rosenzweig, Roy. "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet." *The American Historical Review*, 1998.

Ross, Andrew. 1991. "Hacking away at the counterculture." In *Technoculture*, edited by Constance Penley and Andrew Ross, 107-34. Minneapolis: University of Minnesota Press.

Schultz, Eugene. "Internet Security: Risk Analysis, Strategies, and Firewalls." *Network Security*, vol. 1997, no. 7, 1997, p. 15.

Sterling, Bruce. "Science Fiction And The Internet." *Reading Science Fiction*, 2008, pp. 235–243.

Taddeo, Mariarosaria. "On the Risks of Relying on Analogies to Understand Cyber Conflicts." *Minds and Machines* 26, no. 4 (2016): 317–21.

Warner, Michael. "Cybersecurity: A Pre-History." *Intelligence and National Security*, vol. 27, no. 5, 2012, pp. 781–799.

"Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet." *The American Historical Review*, 1998.

Wolff, Josephine. *You'll See This Message When It Is Too Late: the Legal and Economic Aftermath of Cybersecurity Breaches*. Cambridge: MIT Press, 2018.

Wolfe, Audra J. *Freedoms Laboratory: the Cold War Struggle for the Soul of Science*. Johns Hopkins University Press, 2018.

Zalloua, Zahi Anbra., and Bruce A. Magnusson. *Contagion: Health, Fear, Sovereignty*. Seattle and London: University of Washington Press, 2012.