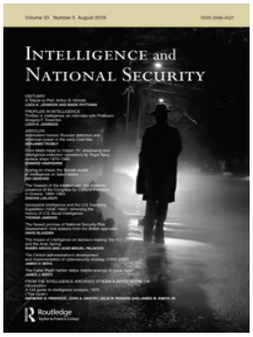

Intelligence and National Security

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

The Clinton administration's development and implementation of cybersecurity strategy (1993–2001)

James D. Boys

To cite this article: James D. Boys (2018) The Clinton administration's development and implementation of cybersecurity strategy (1993–2001), Intelligence and National Security, 33:5, 755-770, DOI: 10.1080/02684527.2018.1449369

To link to this article: https://doi.org/10.1080/02684527.2018.1449369

Published online: 15 Mar 2018.

INTELLIGENCE AND NATIONAL SECURITY, 2018
VOL. 33, NO. 5, 755–770
https://doi.org/10.1080/02684527.2018.1449369

Routledge
Taylor & Francis Group

ARTICLE

The Clinton administration's development and implementation of cybersecurity strategy (1993–2001)

James D. Boys

ABSTRACT

The concept of an assault on the critical infrastructure of the United States is often referred to as a 'Cyber Pearl Harbor'. This implies that such an attack would come as a surprise. By 2016, however, few could claim to be surprised by such an event. This paper explains how the Clinton administration addressed cybersecurity in the 1990s as computers became an everyday item. With the benefits of this era, however, came potentially devastating implications for national security as the Clinton administration was required to confront a form of politically motivated violence unlike any that had been seen before Cyberterrorism.

The potential for a surprise assault on the critical infrastructure of the United States has been described by academics and security analysis as a 'Cyber Pearl Harbor'.[1] The concept of a 'Cyber-Pearl Harbor' is predicated on several factors: Firstly, as Wirtz recently highlighted, that such an attack would be a surprise to policy-makers.[2] Secondly, that it would have a devastating impact upon the United States. Thirdly, that such an attack is feasible. In reality, none of these elements should be taken for granted or assumed to be the case. Not only is there great debate surrounding the viability of such a Digital Day of Infamy, but even the broader concept of cyberterrorism has confounded strategists in their attempts to define the subject, just as policy-makers have struggled to define strategies to safeguard cybersecurity. Although we are now in an era in which computers are ubiquitous, concern over the potential penetration of vital security networks has occupied the minds of analysts for over 50 years as they have sought to appreciate the true scale of the threat posed by this form of terrorism. Appreciating the fact that policy-makers and analysts have feared such an attack for over half a century is vital to any comprehension regarding the nature of the threat posed to cybersecurity and to the national infrastructure of the United States. The role played by individual administrations is also revealing, since the development and implementation of cybersecurity policy has occurred largely out of public view, ensuring a distorted appreciation regarding the relative attention that the subject has received from the political leadership of the United States.

This paper reveals the flaws that exist in the 'Cyber Pearl Harbor' concept of a surprise attack on the US critical infrastructure by revealing the extent to which an effective cybersecurity strategy was developed by the Clinton administration during the 1990s in a specific effort to prevent such an attack. The Clinton administration's foreign policy in general has thus far gone largely under-examined, and its efforts to address challenges to cybersecurity in particular have not been examined in sufficient detail. This has ensured that US efforts to combat cyberterrorism in the 1990s remains something of mystery, further enhancing an orthodox view of the administration as lacking focus on international affairs and

CONTACT James D. Boys james@jamesdboys.com @jamesdboys

the growing threat posed by terrorism. This paper challenges this interpretation to reveal the extent to which the Clinton administration was effectively developing a cybersecurity strategy to address a new and evolving threat to the US critical infrastructure in what it viewed as a productive and effective manner. Through a targeted use of executive orders, presidential directives and the annual national security strategy, the Clinton administration elevated awareness of the issue and drove efforts to address the threat to cybersecurity long before it became a subject of widespread debate, further undermining any suggestion that an attack on the US critical infrastructure could be any sort of a surprise.

The paper utilizes discourse analysis to consider presidential statements and official documents to examine how the Clinton administration developed a cybersecurity strategy during its eight years in office. A deconstruction approach has been adopted to provide a more accurate analysis of the Clinton administration's policies and political initiatives. This approach has been adopted partly due to availability of sources and through a desire to draw upon the administration's own words and policy documentation, rather than on third party interpretations. This enables the analysis to provide a more accurate understanding of both the rhetoric and strategy. It also ensures that a full and detailed appreciation of the program's rationale, instigation, and development can be constructed, free of political or moral perspectives, or the distorting view of hindsight. Once this is revealed, the development of the Clinton administration's efforts to address issues of cybersecurity during the 1990s becomes apparent.

Defining the threats

A major challenge in considering the development and implementation of cybersecurity strategy is the need to define 'cyberterrorism'. This has generally been attempted by seeking to apply concepts of 'terrorism' to the overall area of cyberspace. Terrorism, however, lacks an agreed-upon definition, confounding attempts to adequately define 'cyberterrorism'. Despite this, there have been numerous attempts to define the growing threat to the US critical infrastructure and the broader issue of cyber-threats and cybersecurity, originating from foreign nations, non-state actors, and individuals.

In the year 2000, Dorothy Denning advised the House Armed Services Committee's Special Oversight Panel on Terrorism that cyberterrorism was 'the convergence of terrorism and cyberspace'. Denning argued that to count as cyberterrorism, 'an attack should result in violence against persons or property, or at least cause enough harm to generate fear', which could include 'attacks against critical infrastructures'.[3] Two years previously, Pollitt defined cyberterrorism as 'the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents'. This definition sought to discern between actors and motives, since, for cyberterrorism to have any specific meaning, lawmakers 'must be able to differentiate it from other kinds of computer abuse such as computer crime, economic espionage, or information warfare'.[4]

As with debate surrounding the definition of terrorism, academic disagreement has ensured continuing debate on the merits of cyberterrorism.[5] Jarvis and Macdonald argue that to qualify as cyberterrorism, an attack must have offline or 'real world' consequences that extend beyond damage to information technology.[6] Others have ventured that the use of the expression 'cyberterrorism' is an unhelpful focus on the modus operandi, rather than on the causation or outcome of the crime. Gordon and Ford note, 'We do not use the term "ice pick terrorism" to define bombings of icepick factories, nor would we use it to define terrorism carried out with ice picks'.[7] Joshua Green went further, insisting there

> is no such thing as cyberterrorism – no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer…Which is not to say that cybersecurity isn't a serious problem – it's just not one that involves terrorists.[8]

Compounding the issue of defining cyberterrorism in regards to cybersecurity is the challenge of defining a potential Cyber Pearl Harbor. The concept of a surprise attack on the US critical infrastructure has been referred to by a variety of expressions, including 'electric Pearl Harbor', 'cyber Armageddon', and 'cyber Pearl Harbor'. In their paper, *Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016*, Sean Lawson and Michael K. Middleton detail the development

and usage of the these terms, and the negative implications of the terminology for a balanced debate on the state of US cybersecurity.[9] The term has been utilized for at least 25 years, itself an indication that any such attack could hardly be seen as a surprise anymore. During the past quarter century, the phraseology has evolved, along with attempts to define precisely what it refers to. Winn Schwartau used the phrase twice in 1991, including in testimony before Congress about the threats facing the United States. In an article for *Computerworld* he noted that an 'electronic Pearl Harbor' attack would be 'crippling', and could threaten 'the continuation of well-ordered society'.[10]

The exact understanding of what a Cyber Pearl Harbor would entail has been central to the continuing debate. In 1999, John Markoff explained the impact of such an attack in a *New York Times* article.

> The specter of simultaneous computer network attacks against banking, transportation, commerce and utility targets–as well as against the military–conjures up the fear of an electronic Pearl Harbor in which the nation is paralyzed without a single bullet ever being fired.[11]

The concept of the United States suffering a Cyber Pearl Harbor is one that has been advanced by academics as well as politicians, including former members of the Clinton administration, which was in power when the term was popularized and utilized.

Senator Sam Nunn, who spurned and invitation to serve as Clinton's Defence Secretary, served as the Ranking Minority Member on the Senate Committee on Government Affairs. In its June 1996 hearings into Cyberspace Security, he noted the 250,000 attacks on the Defence Department's information systems that were occurring every year. He questioned how a modern American society would function in the event of a cyber attack if it were left 'without energy, communication, transportation, and financial systems'.[12] The hearings were advised by the Director of Central Intelligence, John Deutch, that the increased 'connectivity and dependency [made the United States] vulnerable to a variety of information warfare attacks'.[13]

Debate over the viability of a cyber attack on US interests has long dominated theoretical debate; the authors of *Computers at Risk* concluded that a 'modern thief can steal more with a computer than with a gun'. It was likely, therefore, that 'tomorrow's terrorist maybe able to do more damage with a keyboard than with a bomb'.[14] In 1993, Arquilla and Ronfeldt made an important distinction between 'netwar' and 'cyberwar'. They argued that the former involved a 'societal-ideational' struggle across networks, while the later was a far more tactical threat to be waged by nation states.[15] Smith, however, directly refuted such suggestions in his article 'An Electronic Pearl Harbor? Not Likely'.[16] These issues were addressed directly by Gompert in *RAND Review*. Was it possible, he asked, that an 'information war [was] being oversold? We don't know'.[17] In 1999 Laqueur concluded that the new Information Age had 'made cyberterrorism possible [ensuring that] the conjunction of technology and terrorism make for an uncertain and frightening future'.[18] A great deal of that uncertainty surrounded the vulnerability of networked computer systems that had become the basis of the nascent Internet during the Clinton administration.[19]

Theoretical basis

To date, the Clinton administration's approach to foreign policy in general, its counterterrorism strategy, and development of an effective cybersecurity strategy, however, has received insufficient attention from academics and researchers. Political opponents have lamented Clinton's time in office as a decade of lost opportunities and confused initiatives, during which the United States lacked purpose and direction, allowing a growing threat to develop.[20] Partly as a result, the orthodox narrative is of an administration that paid scant attention to foreign affairs, and was too busy facing potential removal from office to initiate any meaningful effort to address the growing danger posed to the critical infrastructure. This is unfortunate, as an examination of cybersecurity strategy as developed and implemented by the Clinton administration reveals a White House that quickly recognized the growing threat and moved to implement policies to address them. A consideration of the time also reveals the extent to which these strategies were faced by bureaucratic resistance that hindered their implementation. Since studies of

the Clinton White House have so far failed to consider its development of cybersecurity strategies, the administration's efforts remain misunderstood and their lasting impact under-appreciated. This has been exacerbated by former members of the administration, who have failed to explain their attempts to address issues of cybersecurity in their memoirs.

Although too little attention has been paid so far to the Clinton administration's efforts to combat international terrorism in general, or its efforts to address cybersecurity in particular, this is not to suggest that nothing has been written on the situation. There is, however, no defining work on cybersecurity strategy as devised by the Clinton White House, and certainly none that has focused exclusively on its efforts to combat cyberterrorism. The small number of books that have been produced on the administration's foreign policy in general have failed to present a thorough analysis of the administration's policies initiatives. Both William G. Hyland's *Clinton's World* and John Dumbrell's *Clinton's Foreign Policy* were early assessments of the Clinton administration's foreign policy, but neither address its development and implementation of cybersecurity strategy.[21] Richard T. Sale's *Clinton's Secret Wars* is an excellent examination of the use of force by the administration, but also excludes a consideration of its evolving cybersecurity strategy.[22] The Clinton administration's attempt to address counterterrorism in general, as well as its cyberterrorism strategy, was addressed by Chin-Kuei Tsui's *Clinton, New Terrorism and the Origins of the War on Terror*.[23] However, the approach taken here focuses on issues of rhetoric, not policy, ensuring that this remains an interesting, if frustrating text for those seeking enlightenment on the actual development of strategy in the 1990s.

This oversight has been reflected in the memoirs written by the senior members of the Clinton administration's national security team, including Bill Clinton's *My Life*, Warren Christopher's *Chances of a Lifetime,* Madeleine Albright's *Madame Secretary*, Nancy Soderberg's *Superpower Myth* and Anthony Lake's *Six Nightmares*.[24] The one former member of the Clinton administration who has written on the subject is Richard A. Clarke, whose texts *Against all Enemies,* and *Cyber War*, should be considered essential reading for anyone seeking an insight into the development of policy during this era.[25] Clarke's analysis of cybersecurity, however, is hindered by his presentation of potential future scenarios, rather than an analysis of actual events and policy developments, a stylistic choice that undermines the academic and political significance of the work.

Whereas a limited range of material is available that addresses the Clinton administration's overall foreign policies, academic articles on US efforts to address cyberterrorism and threats to US cybersecurity have been slow to address its evolution prior to 11 September 2001. Instead, articles have offered a broad overview of cyberterrorism, with brief references to the pre-9/11 era that treat the time as a precursor to the eventual War on Terror as launched by President George W. Bush. Examples include Michael Warner's 'Cybersecurity: A Pre-History', Myriam Dunn Cavelty's 'Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Gabriel Weimann's 'Cyberterrorism: The Sum of all Fears?' and Maura Conway's 'Cyberterrorism: Hype and Reality'.[26] One text that addresses the emerging threat to cybersecurity in detail is Julian Richards' *Cyber-War: The Anatomy of the Global Security Threat*. Drawing upon a career in signals intelligence, the text adopts what the author acknowledges to be a 'critical view about the threat of cyber war'.[27] As with other material on cyber-terrorism, however, this text also manages to address developments prior to 1992 and a great deal after 2001, but fails to consider what was occurring in the eight years prior to 11 September 2001.

This paper addresses the gap in the literature as it currently stands. The Clinton administration's development and implementation of a cybersecurity strategy as a tool of US counterterrorism strategy has not figured in an appreciation of how the nation addressed the growing dangers, or in any successful consideration of the evolution of policy after the attacks of 2001. The paper addresses this omission through a discourse analysis drawing from an extensive range of available materials. The passage of time has enabled an extensive range of primary sources to emerge from the Clinton Library in Little Rock, Arkansas, including presidential speeches, statements and official documents from the National Security Council, many of which have only recently been declassified. These have been compounded by the use of respected secondary sources to ensure the use of the most effective sources available.

This paper utilizes discourse analysis to accurately analyze the precise terminology and exact wording used by the Clinton administration in regard to its development and implementation of a cybersecurity strategy. In 1993, Doty noted that discourse analysis was a 'system of statements in which each individual statements makes sense', however, it also produces interpretative possibilities.[28] This paper concedes that while language is crucial to the notion of discourse, political and social life is not reducible to language or linguistic analysis alone and that problems certainly do exist within this analytical approach. In 1994, George observed that studies of discourse analysis were united by a commitment to understanding how 'textual and social processes are intrinsically connected and to describe, in specific contexts, the implications of this connection for the way we think and act in the contemporary world'.[29] This paper focuses on the statements and documentation produced by Clinton administration officials as they sought to address the evolving threat to the US critical infrastructure.

Since policy implementation traditionally follows policy pronouncements, discourse analysis aides in an appreciation of the extent to which the words spoken by administration officials impacted the direction of policy and its implementation during its eight years in office. In 1998, Weldes observed that studying political language is vital since it 'actively produces the issues with which policy-makers deal and the specific problems that they confront'.[30] Selection bias is clearly a challenge in any use of discourse analysis. Accordingly, in selecting material, this paper has carefully drawn on the specific words of Clinton administration officials, rather than on material that maybe interpreted by third parties. Where material has been drawn from contemporary reportage, it is to convey the words of campaign officials, not journalists. A consideration of this material reveals the extent to which the Clinton administration successfully developed cybersecurity strategies as part of its evolving counterterrorism program between 1993 and 2001. This paper will consider the changing definition of cyberterrorism and of cybersecurity and its development throughout the computer-age, before evaluating the Clinton administration's efforts to devise cybersecurity policies and practices during its eight years in office.

The evolving cybersecurity policy response

Issues of cybersecurity were apparent almost as soon as computers were capable of being brought together in networks. Two major concerns quickly emerged; the potential threat to national security, and the implications civil liberties from unauthorized access to government systems. As early as 1966, the House of Representatives held hearings into the potential risks that networked machines could pose for individual liberties and freedoms.[31] Four years later the RAND Corporation concluded that it was 'unwise to incorporate classified or sensitive information in a system functioning in an open environment unless significant risk of accidental disclosure can be accepted'.[32] Fears existed over the risks of miscalculation and human error in handling such technology. In 1979 a NORAD exercise mistakenly triggered reports of an incoming Soviet missile that reached to the highest levels of the national security council.[33] Even earlier, in October 1962, radar operators mistakenly believed that the Soviet Union had initiated a launch at the height of the Cuban Missile Crisis when an exercise tape was incorrectly fed into a computer.[34]

By 1983, the Department of Defense was 'increasingly concerned about [the] future security' of its networked computer systems, leading the *New York Times* to conclude that 'a volatile mix of technical and social trends…bodes ill for the future'.[35] The combination of concerns regarding civil liberties and national security was addressed in National Security Decision Directive (NSDD)-145. Dated September 27, 1984, 'National Policy on Telecommunications and Automated Information System Security', concluded that US systems were 'highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation'. It concluded that the technology needed to exploit them was 'used extensively by foreign nations and [could] be employed, as well, by terrorist groups and criminal elements'.[36] The directive assigned the responsibility for network oversight to the National Security Agency (NSA), a move that was attacked as being 'an unprecedented and ill-advised expansion of the military's influence in [US] society'.[37] Eventually, the Computer Security Act of 1987 divided oversight of federal computer systems between the NSA, which would monitor national security networks, and

the National Bureau of Standards (NBS), which was to be responsible for all other systems. It was clear by the mid-1980s, that 'unfriendly governments and terrorist organizations [were] finding easy pickings' among networked computer systems in the United States.[38] As noted by Sir David Omand and Mark Phythian, however, the debate surrounding unauthorized access to government systems and the implications for civil liberties is far from over, as 'the role and activities of national intelligence agencies could themselves represent the problem or obstacle in the way of securing human rights'.[39]

By the start of the 1990s, the National Academy of Sciences warned that the nation's increasing dependency on computers meant the United States was increasingly vulnerable, 'to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack'.[40] These concerns were addressed by the George H. W. Bush administration in NSD-42, 'National Policy for the Security of National Security Telecommunications and Information Systems', dated 5 July 1990. The directive recognized the susceptibility of networked computer systems to 'interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat'. The directive rescinded Reagan's NSDD-145 and established the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This body was tasked with considering technical matters and developing policies, procedures, guidelines, and instructions under guidance from the National Security Council/Policy Coordinating Committee (PCC) for National Security Telecommunications.[41]

The Clinton administration and the developing cybersecurity threat

The Clinton administration took office at a time of geopolitical upheaval. The Cold War that had dominated international relations for decades had ended, the Soviet Union had collapsed, Germany had reunified and South Africa would soon elect Nelson Mandela as president. These historic events, and the development of globalization presented both challenges and opportunities for the incoming Clinton administration and for American citizens. The changing international environment presented an opportunity for the new White House national security team to redefine US grand strategy. Having been focused on the military threat posed by the Warsaw Pact throughout the Cold War, US security strategy could now be re-designed to account for the new realities of the era through which the Clinton administration would govern.

In its annual National Security Strategy, the Clinton White House detailed three central pillars: enhanced national security, the need for economic security, and democratic promotion. The changed geo-political era allowed for this development, along with the personal predilections of the president and his key advisers. Vice President Gore was a strong advocate of the Trade, Prosperity and Peace strategy originally espoused in the 1930s by his fellow Tennessean, Cordell Hull. This found favor with President Clinton whose main exposure to international relations prior to his election had been in regard to trade and exports from his native Arkansas. Finally, the Kantian concept of Democratic Peace had become feasible with the end of the Cold War, ensuring its place within Clinton's Grand Strategy.[42] In addition to these three central pillars of national security strategy, the Clinton administration identified a series of strategic hazards to be addressed, including the transnational threat posed by challenges to US cybersecurity.

By January 1993, it was apparent that the technology that promised to make life easier for all Americans also presented great opportunities to those who wished to wreak havoc on the world's only remaining superpower. It quickly became apparent that there was a dark side to the new era of globalization, requiring the term 'cyber attack' to be introduced into the presidential lexicon.[43] The risk posed by a cyber attack was not only to sensitive data stored on networked computer systems, but also to command and control functions that coordinated critical infrastructure architecture, including air traffic control and national defense systems.

As early as 1995, the Clinton administration recognized that the 'threat of intrusions to our military and commercial information systems [posed] a significant risk to national security and must be addressed'.[44] From 1998, the specific threat posed to cybersecurity was identified in the annual National

Security Strategy, since attacks on the information infrastructure, 'ranging from cyber-crime to a strategic information attack on the United States via the global information network, present a dangerous new threat to [US] national security'.[45] The White House warned that cyber attacks 'could originate from terrorist or criminal groups as well as hostile states'.[46] The administration recognized that 'other governments and terrorist groups are creating sophisticated, well-organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depend on them'.[47]

The Clinton administration also sought to counter the danger to cybersecurity in a series of executive orders, drawing upon presidential authority detailed in existing statutes, and the Constitution of the United States.[48] Executive Order 12864, dated September 1993, established the United States Advisory Council on the National Information Infrastructure. The council's remit was to advise on the development of the National Information Infrastructure, defined as, 'the integration of hardware, software, and skills that will make it easy and affordable to connect people with each other, with computers, and with a vast array of services and information resources'. As befits the timing of the document, the words 'Internet' or 'World Wide Web' do not appear. At that stage, the concept of what a 'National Information Infrastructure' would entail was undetermined, with the council assigned the task of its development, evolution, and the role to be played by the private and public sectors. Although key economic questions regarding the potential for job creation, economic growth, and increased productivity were to be addressed, so too were the vital issues of 'national security, emergency preparedness, system security and network protection implications'. Even before the Internet had entered into the public consciousness, therefore, the Clinton administration begun to consider the risks associated with such a computer network. Based on authority granted under the Constitution, the Federal Advisory Committee Act, and section 301 of title 3, United States Code, the order restricted membership of the council to less than 25 members, to be appointed by the Secretary of Commerce for an initial period of two years.[49] A little under a year later, on 19 August 1994, President Clinton signed Executive Order 12924 to address the expiration of the Export Administration Act of 1979. The order noted that 'the unrestricted access of foreign parties to US goods, technology, and technical data…constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States'.[50]

On 15 July 1996, Executive Order 13010 was signed, which focused on Critical Infrastructure Protection. The document acknowledged that the national infrastructure was already so vital to the defense and economic security of the United States that its disruption would have a 'debilitating impact' on the nation. This was understood to cover potential attacks on water supplies, electrical systems, financial services, fuel depots, transportation hubs, telecommunications systems, and the continuity of government. The White House noted that the potential risks to these systems could be categorized as either physical threats, or cyberthreats. Due to the fact that so many of these aspects of national life were operated by the private sector, the order established the Infrastructure Protection Task Force (IPTF) in an effort to 'identify and coordinate existing expertise, inside and outside of the Federal Government' with a view to establishing a partnership between the government and business. The executive order also established the President's Commission on Critical Infrastructure Protection, designed to report upon the risks that existed, the vulnerability of vital systems, liaise between public and private sector operators, and finally, to 'recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyberthreats and assuring their continued operation'.[51]

Executive Order 13026, dated 15 November 1996 which directly addressed the administration of Export Controls on Encryption Products. Issued days after the president's re-election, the order was designed 'to provide for appropriate controls on the export and foreign dissemination of encryption products [that] could harm national security and foreign policy interests even where comparable products are or appear to be available from sources outside the United States'.[52]

The Clinton administration issued two further related executive orders during its second term, as the Internet became part of everyday culture and the accompanying threats to national security became apparent. Executive Order 13035, dated 11 February 1997 established the Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next-Generation

Internet. Drawn from a variety of sectors, the committee was tasked with assessing the 'progress made in implementing the High-Performance Computing and Communications (HPCC) Program' and in 'designing and implementing the Next Generation Internet initiative'. The initiative was, at least in part, designed to ascertain 'whether the research and development undertaken pursuant to the HPCC Program is helping to maintain United States leadership in advanced computing and communications technologies and their applications'.[53]

If the aforementioned documents helped establish the basis for what became the Internet, Executive Order 13133, dated August 1999, addressed the emerging threats that this technology posed. It established a new Working Group on Unlawful Conduct on the Internet to report on the viability of existing legislation to address the policing of the Internet. Though not specifically tasked with targeting terrorist groups, the group was charged with reporting on

> the extent to which existing Federal laws provide a sufficient basis for effective investigation and prosecution of unlawful conduct that involves the use of the Internet, such as the illegal sale of guns, explosives, controlled substances, and prescription drugs, as well as fraud and child pornography.[54]

Finally, a series of presidential directives were issued by the Clinton administration to address issues of cybersecurity and the threats posed to the national critical infrastructure. Presidential Decision Directive (PDD) 5, dated April 1993, addressed 'Public Encryption Management'. It was designed to focus on the need for encryption to secure financial transactions and communications, as well as concerns that encryption could be used to 'frustrate lawful government electronic surveillance'. This was a potential problem for domestic law enforcement, as well as for US foreign policy decision-makers, since encryption technology, when used abroad, could 'be used to thwart foreign intelligence activities critical to [US] national interests'. The Clinton administration acknowledged that encryption technology required 'new, innovative approaches' to enabling the security services to defend the nation while ensuring that privacy and civil liberties were not curtailed.[55] The findings of PDD-5 were referenced in Presidential Review Directive (PRD) 27, also signed in April 1993, entitled *Advanced Telecommunications and Encryption*. It noted the urgent need to 'accommodate the government's interests in law enforcement, privacy, national security, productivity and competitiveness'.[56] Signed by National Security Adviser Anthony Lake, the directive initiated a study into how encryption technology could impact law enforcement initiatives and intelligence gathering operations.

On 22 May 1998, the 18-page PDD-63 *Critical Infrastructure Protection* emerged as the Clinton administration's most comprehensive document on the issue of cybersecurity. The directive established a Senior Directorate for Infrastructure Protection on the National Security Council staff, in an effort to 'eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems'. The directive also established the office of National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, tasked with chairing the Critical Infrastructure Coordination Group (CICG); reporting to the Deputies Committee of the NSC; and providing budgetary advice to ensure the protection of the critical infrastructure.[57] As initially held by Richard Clarke, this ensured that, in theory, the full power of the federal government was available, 'to ensure that critical infrastructure protection is achieved and maintained'. In practice, however, the bureaucratic limitations of the role ensured that the directive 'made clear … that the czar could not direct anyone to do anything'.[58]

PDD-63 referred to the threat of cyber-warfare, noting that adversaries may seek alternative forms of attack to by-pass the military superiority of the United States. Indeed, it was feared that 'non-traditional attacks on our infrastructure and information systems maybe capable of significantly harming both our military power and our economy'. As the first administration to place national economic security at the heart of its grand strategy, it was not surprising that the Clinton White House appreciated the potential dangers that were posed by an attack on the US economy via cyberspace.

The bureaucratic response to cybersecurity

In March 1993, Colin Powell, Chairman of the Joint Chiefs of Staff, issued a policy memo reflecting the Clinton administration's objectives regarding information warfare, defined as the preparedness to

'decapitate the enemy's command structure from its body of combat forces'.[59] Much of the implementation of the Clinton administration's cybersecurity strategies involved the US military, which had steadily increased its cyber-related capacities. The Air Force Electronic Warfare Centre had been re-designated as the Air Force Information Operations Centre in September 1993, drawing together experts from the department's Intelligence Command and Cryptology Support Centre.[60] The Navy Information Warfare Activity facility opened at Fort Mead in 1994, and in 1995 Army Land Information Warfare Activity commenced, as the first officers specifically trained in cyber warfare graduated from the National Defense University.

On 28 February 1994, the Joint Security Commission that the Clinton administration had established the previous year, reported to the Secretary of Defense and the Director of Central Intelligence that information systems technology was evolving much faster than information systems security technology. Overcoming this gap, the commission concluded, required 'careful threat assessments, well-thought-out investment strategies, sufficient funding, and management attention'. If this did not occur, 'the confidentiality, integrity, and availability of [US] classified and unclassified information assets' would be at risk.[61] Among the commission's recommendations were for policy formulation to be consolidated under a joint Pentagon/CIA executive committee, and for the development of a cost effective information systems security investment strategy. Finally, the commission called for the National Security Agency to be designated as the executive agent for systems security research and development, covering classified and unclassified information.[62]

These bureaucratic responses were necessary, since the United States had 'neither come to grips with the enormity of the problem nor devoted the resources necessary to understand fully, much less rise to, the challenge'.[63] This prompted the US Air Force to release 'Cornerstones of Information Warfare', on the potential of using computers to attack other computers, while the RAND Corporation was tasked with identifying weaknesses in the Pentagon's IT systems. The report's findings confirmed fears that the US homeland 'may no longer provide a sanctuary from outside attack'.[64] This was reinforced by the General Accounting Office (GAO), which acknowledged that the Pentagon's information systems were being attacked up to 250,000 times a day.[65] The Director of the US Department of Defense information System Security program, Robert Ayres, revealed that Pentagon computer systems had been successfully penetrated 250,000 times in 1995.[66] The Clinton White House recognized that 'catastrophic damage' was inevitable if 'foreign nationals or terrorists could use "information warfare" techniques to disrupt military operations by harming command and control systems, the public switch network, and other systems or networks Defense relies on'.[67]

This was not just a challenge for the Pentagon, however, as the Clinton administration briefed Congress on the gathering threat posed to cybersecurity. In February 1996, it dispatched DCI John Deutch to brief the US Senate Select Committee on Intelligence. He warned that US agencies had 'identified a handful of countries' that had 'instituted formal information warfare programs' against the United States. Deutch conceded that the threat to US information systems would 'grow in coming years' as 'more countries and groups develop new strategies that incorporate such attacks'.[68] Four months later he advised the Permanent Subcommittee on Investigations of the United States' Senate Governmental Affairs Committee that international terrorist groups already had 'the capability to attack the information infrastructure of the United States, even if they use relatively simple means'.[69] The following month, in July 1996, Deputy Attorney General Jamie S. Gorelick, briefed the Senate that although the United States had 'not yet had a terrorist attack on the infrastructure', she feared that such an assault was 'a present threat'. She noted, 'We do not want to wait for the cyber equivalent of Pearl Harbor, before we wake up to the threat and take steps to confront it'.[70]

As the Clinton administration's first term in office came to a close, it was clear that the executive branch agencies; the Pentagon, the CIA, the GAO, as well as the White House, recognized the challenges posed by the growing system of networked computers. These networks promised to make life easier and more enjoyable for Americans, yet simultaneously threatened to expose the United States to a devastating assault upon its critical infrastructure, in a potential attack that members of the Clinton administration were already beginning to compare to the previous attack at Pearl Harbor.

Securing the critical infrastructure

Although the Department of Homeland Security did not come into existence until after the attacks of 11 September 2001, the conceptual thinking behind it had its origins, in part, in the 1995 destruction of the Alfred P. Murrah Building in Oklahoma City. This attack, at the time the largest single terrorist incident in US history, began the process of drawing together key aspects to form the federal protection of critical infrastructure; cyberthreats, infrastructures, terrorism, and asymmetric vulnerability.[71]

Two months after the bombing, President Clinton established the inter-agency Critical Infrastructure Working Group (CIWG). Tasked with studying the vulnerabilities of the United States' critical infrastructure to potential attack, the CIWG's January 1996 report resulted in the issuing of Executive Order 13010 and the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP). Headed by retired Air Force General Robert Marsh, the PCCIP concluded that the resources needed to devastate the US critical infrastructure were 'inexpensive, readily available, and easy to use.[72] In its final report, dated October 1997, the PCCIP noted that the evolution in technology that was being enjoyed by Americans was being manipulated by enemies of the state, ensuring that a 'personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to cause harm'.[73] The report concluded that 'the security, the economy, the way of life, and perhaps even the survival of the industrialized world were dependent on the triad of electrical power, communications, and computers'.[74] Despite being launched in the wake of the attack in Oklahoma City, the PCCIP did not focus on right-wing groups, or international networks, but instead addressed the threat to the nation's critical infrastructure from nation states and the need to create public-private partnerships to address the situation.

The recommendations and focus of the PCCIP report were incorporated into PDD-63, signed by President Clinton in May 1998. At the heart of this presidential directive was the creation of the several entities. The National Infrastructure Protection Centre (NIPC), based at the FBI, was tasked with serving as the 'national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity'. Designed to be linked to the rest of the federal government, the inter-agency NIPC was intended to provide 'timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response'. In an attempt to overcome the bureaucratic resistance that existed between competing executive branch agencies, the Clinton administration ordered that all agencies 'cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law'.[75] The 1998 document, *Terrorism in the United States,* issued by the Department of Justice's Counterterrorism Threat Assessment and Warning Unit, insisted that the NIPC was 'forging the analytical, information-sharing, investigative, and warning capabilities necessary to confront the terrorist threats of the twenty-first century'.[76]

Secondly, PDD-63 established the Information Sharing and Analysis Centre (ISAC) to enable private enterprise to work with the federal government in a joint attempt to secure critical infrastructure. In a development that became viewed as the 'securitization of cyberspace' the federal government initiated efforts to further secure the US critical infrastructure architecture from threats posed by foreign nations, as well as a growing list of non-state actors. These moves required the acquiescence of private organizations, responsible for the day-to-day operations of such entities, to work with the government in the national interest of the United States.[77]

War-games and horizon scanning

A series of initiatives were launched during the second term of the Clinton administration to ascertain the extent to which the US critical infrastructure was susceptible to external penetration. Between 9 June and 13 June 1997, a group of operatives from the National Security Agency stress-tested cyber-security at the Pentagon in an operation codenamed *Eligible Receiver 97*. The initiative successfully accessed supposedly secure networks using freely available software, and within a two-day period, highlighted deficiencies in local, state and federal government systems, including the National Command

Authority. The system-wide failings led to an immediate order for intrusion detection software across the Department of Defence, an acknowledgment that the operation 'succeeded beyond its planner's wildest dreams in elevating the awareness of threats to our computer systems'.[78]

In 1998 and 1999, the same systems came under attack once more, but this time from outside sources. In 1998 Ehud Tenenbaum, a nineteen-year old Israeli, along with two Californian teenagers, accessed systems at NASA, the US Air Force, the US Navy, and the Pentagon. The subsequent government investigation, codenamed *Solar Sunrise*, revealed how porous the systems remained. This was confirmed the following year when operation *Moonlight Maze* was launched by the FBI to investigate what appeared to be a coordinated, continuous penetration of US networks that lasted for more than two years, and which stopped as suddenly as it started, with no indication as to who was responsible. At the time, *Moonlight Maze* was the most wide-ranging digital investigation ever launched, with up to 100 agents involved and which also drew on the assistance of GCHQ in the UK.[79] In response to concerns raised by the results of *Eligible Receiver*, as well as the findings of the PCCIP, the Clinton administration launched the National Domestic Preparedness Office (NDPO) in October 1998. Designed as an attempt to coordinate the growing number of federal agencies with responsibilities in the event of a terrorist incident, the NDPO was 'an information clearinghouse', to facilitate assistance in time of national emergency.[80]

These initiatives; the NDPO, ISAC, NIPC, and Richard Clarke's appointment as National Coordinator for Security, Infrastructure Protection, and Counterterrorism, all formed part of the Clinton administration's efforts to counter the growing threat of cyber-attacks and fears of a potential cyber Pearl Harbor, which found focus around the end of the century celebrations. Although the much-anticipated cybersecurity crisis on Millennium Eve failed to occur, a series of high profile online sites were targeted by hackers early in the year 2000, leading to the first White House conference on cybersecurity. Neither the Clinton administration, nor the business sector, however, wished to see the issue of cybersecurity regulated. The dynamics of the moment also impacted any chance for progress: The administration was running out of time, congress was not inclined to legislate on the issue, and business leaders were wary of any developments that placed restrictions on trade or earnings.

The Clinton administration released the *National Plan for Information Systems Protection* in January 2000, which highlighted the severity of the threat posed to cybersecurity. The report stressed that whatever response was initiated, must not come at the expense of civil liberties, for as President Clinton observed as he unveiled the report, it was 'essential that we do not undermine liberty in the name of liberty'.[81] In doing so, President Clinton was making a tactic acknowledgment that this had occurred previously, as first amendment rights had been suspended during World War I, as the US campaigned to make the world safe for democracy, and that Japanese-Americans had been held in internment camps in the aftermath of the attack on Pearl Harbor.

The *National Plan for Information Systems Protection* included proposals for an Institute for Information Infrastructure Protection, to bring together computer scientists and engineers to address the challenges posed to cybersecurity. This, and other such developments, were to be paid for from a $91 million package, which formed part of $2 billion allocated for new security challenges in the Clinton administration's final budget. The document acknowledged that this was the beginning of a process, which required collaboration and a dialog with government and experts in the developing field, and that any plan for cyber defense would need to 'evolve and be updated' as vulnerabilities and threats emerged. This was, however, the first such attempt to devise a way to safeguard cyberspace and was enacted as the administration prepared to leave office, with rapidly diminishing political capital.

The Clinton administration's legacy in the area of Cyber, however, was clouded by Vice President Gore on 9 March 1999. Interviewed by Wolf Blitzer on *CNN* and asked to distinguish himself from his rival, Senator Bill Bradley, Gore noted 'During my service in the United States Congress, I took the initiative in creating the Internet'. The backlash to this statement, repeatedly presented as Gore claiming to have 'invented' the Internet, led Internet pioneers Robert Kahn and Vinton Cerf to write an open letter in his defense. They insisted that Gore was 'the first political leader to recognize the importance of the Internet and to promote and support its development' and that 'No other elected official, to our knowledge, has made a greater contribution [to the Internet] over a longer period of time'. Despite these efforts,

the damage to Gore's credibility was done, as he established a reputation for embellishment, rather than initiative, proving detrimental not only to his own presidential aspirations, but also to the lasting impression of the Clinton administration's efforts in this vital policy area.[82]

Conclusion

The perceived risks to the United States from an attack on its critical infrastructure are often referred to as a potential Cyber-Peal Harbor. Clearly, however, this analogy is far from accurate, since the threat posed by such an attack has been considered for decades and a successive number of administrations, including that of Bill Clinton, have sought to address the evolving risks associated with such an assault. Debate continues as to the appropriateness of this phrase, such an attack could hardly be seen as having been un-foreseen, its potential impact on the nation is disputed, and its technical feasibility is in dispute. Even the basis tenets of the analogy are debatable, since the potential for an attack on US interests in the Pacific had been anticipated and factored into strategic thinking prior to December 1941, and that despite the loss of life, the events of that day failed to prove catastrophic to the United States, or its interests.

The Clinton administration coincided not only with the end of the Cold War and the rise of globalization, but also the rise of the dark side of globalization, manifested in the threats to the developing US critical infrastructure system, a network that simultaneously streamlined services to enhance American lives, while also providing an all-too tempting target for those seeking to cripple the nation. During its eight years in office, the Clinton administration made repeated use of national security strategy reports, presidential directives, and executive orders in an attempt to prevent attacks on the US critical infrastructure. As he prepared to leave office, in December 2000, President Clinton listed cybersecurity as one of the five key policy areas for the United States to address in the years ahead, along with the challenges posed by AIDS, maintaining the NATO alliance, regional conflicts and future dealings with Russia and China.[83] The administration's efforts to safeguard this vital national asset, though stymied by bureaucratic resistance on occasion, proved the basis for policies that evolved long after it left office and which continue to provide defenses in the twenty-first century. Over seventeen years later, therefore, it is clearly not appropriate to discuss a potential attack as a 'Cyber-Pearl Harbour'. If and when such an attack comes, it will be no surprise.

Notes

1. Schwartau, *Information Warfare*, 43. The term 'Digital Pearl Harbor' is also used, at times inter-changeably. See Richards, *Cyber-War*, 21.
2. Wirtz, "The Cyber Pearl Harbor".
3. Denning, "Cyberterrorism". See also Denning, "Cyberwarriors".
4. Pollitt, "Cyberterrorism".
5. Devost, Houghton, and Pollard, "Information Terrorism".
6. Jarvis and Macdonald, "What is Cyberterrorism".
7. Gordon and Ford "Cyberterrorism?".
8. Green, "The Myth of Cyberterrorism".
9. Lawson and Middleton, "Cyber Pearl Harbor", https://www.seanlawson.net/wp-content/uploads/2017/02/LawsonMiddleton-CyberPearlHarborEssay.pdf.
10. Schwartau, "Fighting Terminal Terrorism," 23.
11. Markoff, "Blown to Bits".
12. Opening statement of Senator Sam Nunn, Ranking Minority Member, Senate Permanent Subcommittee on Investigations, Hearing on Security in Cyber Space, June 5, 1996.
13. John M. Deutch, 'Foreign Information Warfare Programs and Capabilities', Testimony to the U.S. Senate Committee on Governmental Affairs; Permanent Subcommittee on Investigations, June 25, 1996.
14. National Academy of Sciences, *Computers at Risk*, 7.
15. Arquilla and Ronfeldt, "Cyberwar is Coming!"
16. Smith, "An Electronic Pearl Harbor?".
17. Gompert, "Keeping Information Warfare in Perspective".

18. Laqueur, *The New Terrorism*, 254.
19. For more attempts to define cyberterrorism see Weimann, "Cyberterrorism"; Hua and Bapna, "How Can We Deter Cyberterrorism?"; and Conway, "Cyberterrorism".
20. For critical analysis of the Clinton administration's foreign policy initiatives, see Hyland, *Clinton's World*; Miller, "The Clinton Years"; Mandelbaum, "Foreign Policy as Social Work"; Muravchik, "Carrying a Small Stick"; Hyland, "A Mediocre Record"; and Ullman, "A Late Recovery".
21. Hyland, *Clinton's World*; and Dumbrell, *Clinton's Foreign Policy*.
22. Sale, *Clinton's Secret Wars*.
23. Tsui, *Clinton, New Terrorism*.
24. See Clinton, *My Life*; Christopher, *Chances of a Lifetime*; Albright, *Madame Secretary*; Soderberg, *Superpower Myth*; and Lake, *Six Nightmares*.
25. Clarke, *Against all Enemies*; and Clarke and Knake, *Cyber War*.
26. Warner, "Cybersecurity"; Dunn Cavelty, "Cyber-Terror-Looming Threat or Phantom Menace?"; Weimann, "Cyberterrorism"; and Conway, "Cyberterrorism: Hype and Reality".
27. Richards, *Cyber-War*, 6.
28. Doty, "Foreign Policy as Social Construction," 297–320.
29. George, *Discourses of Global Politics*.
30. Weldes, "Bureaucratic Politics," 216–225.
31. US House of Representatives, Committee on Government Operations, 'The Computer and Invasion of Privacy', hearings held July 26–28, 1966, 89th Congress, Second Session.
32. 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, February 11, 1970.
33. Gates, *From the Shadows*, 114. President Reagan viewed *Wargames* at the White House and subsequently raised its central premise in meetings with members of Congress. See Cannon, *President Reagan*, 38.
34. Sagan, *The Limits of Safety*, 238–41.
35. Broad, "Computer Security Worries Military Experts".
36. NSDD-145, "National Policy on Telecommunications and Automated Information System Security," September 17, 1984.
37. Congressman Jack Brooks (D-TX), quoted in Goldberg, "The National Guards".
38. Goldberg, "The National Guards," 44–6; Greenhouse, "Computer Security Shift is Approved by Senate".
39. Omand and Phythian, "Ethics and Intelligence," 41.
40. National Academy of Sciences, *Computers at Risk*, 7.
41. NSD-42, "National Policy for the Security of National Security Telecommunications and Information Systems," 5 July 1990.
42. See Boys, *Clinton's Grand Strategy*.
43. *Public Papers of the President, William Jefferson Clinton,* (1998), vol. 1, Commencement Address at the United States Naval Academy in Annapolis, Maryland, May 22, 1998, 826.
44. *National Security Strategy of the United States, 1995*, 8.
45. *National Security Strategy of the United States 1998*, 6.
46. *National Security Strategy of the United States 1999*, 2.
47. Ibid., 17.
48. Specifically, the United States Constitution, the Federal Advisory Committee Act, as amended (5 U.S.C. App. 2), and section 301 of title 3, United States Code.
49. Executive Order 12864 of September 15, 1993, "United States Advisory Council on the National Information Infrastructure", *Federal Register* 58, no. 179 (September 17, 1993). Membership of the United States Advisory Council on the National Information Infrastructure was raised to 30 on December 30, 1993 by Executive Order 12890, and to 37 six months later on June 13, 1994 via Executive Order 12921. The Council concluded its work and its remit was revoked by Executive Order 13062, dated October 2, 1997. The National Infrastructure Advisory Council was later constituted under President George W. Bush under Executive Order 13231, dated October 16, 2001.
50. Executive Order 12924 of August 19, 1994, "Continuation of Export Control Regulations," *Federal Register* 59, no. 162 (August 23, 1994), 43437.
51. Executive Order 13010 of July 15, 1996, "Critical Infrastructure Protection," *Federal Register* 61, no. 138, (July 17, 1996), 37347–50.
52. Executive Order 13026 of November 15, 1996, "Administration of Export Controls on Encryption Products," *Federal Register* 61, no. 224 (November 19, 1996), 58767–8.
53. Executive Order 13035 of February 11, 1997, "Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet," *Federal Register* 62, no. 31 (February 14, 1997), 7131.
54. Executive Order 13133 of August 5, 1999, "Working Group on Unlawful Conduct on the Internet," *Federal Register* 64, no. 154 (August 11, 1999), 43895.
55. Presidential Decision Directive-5, "Public Encryption Management," April 15, 1993.

56. Presidential Review Directive-27, "Advanced Telecommunications and Encryption," April 16, 1993.
57. Presidential Review Directive -63, "Critical Infrastructure Protection," May 22, 1998.
58. Clarke and Knake, *Cyber War*, 108.
59. Colin Powell, Memorandum of Policy 30, "Command and Control Warfare," March 8, 1993.
60. This wing of the Air Force underwent several re-designations in the early twenty-first century, before becoming the 688th Cyberspace Wing, on September 13, 2013.
61. Joint Security Commission, *Redefining Security*, vii.
62. Ibid., 107–10.
63. Ibid., 2.
64. Molander, Riddile, and Wilson, *Strategic Information Warfare*, xi, xvii, 3, 9, 31. See also Warner, "Cybersecurity".
65. Warner, "Cybersecurity," 795.
66. Ayers, "The New Threat," 23.
67. US Congress, General Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," Technical Report GAO/AIMD-96-84, May 22, 1996.
68. John M. Deutch, "Worldwide Threat Assessment Brief to the Senate Select Committee on Intelligence," February 22, 1996.
69. John M. Deutch, statement before the US Senate Governmental Affairs Committee (Permanent Subcommittee on Investigations), June 25, 1996.
70. Jamie S. Gorelick, Deputy Attorney General, Statement to US Senate, Committee on Government Affairs, Permeant Subcommittee on Investigations, Hearing on 'Security on Cyberspace,' 104th Congress, 2nd Session, July 16, 1996.
71. Dunn and Wigert, *The International CIIP Handbook 2004*. See also Dunn Cavelty, *Cyber-Security and Threat Politics*, 10.
72. President's Commission on Critical Infrastructure Protection, Final Report, *Critical Foundations: Protecting America's Infrastructure,* (October 1997), 14.
73. President's Commission on Critical Infrastructure Protection, Final Report, *Critical Foundations: Protecting America's Infrastructure* (October 1997), x.
74. Cavelty, *Cyber-Security and threat Politics,* 10.
75. Presidential Review Directive-63, "Critical Infrastructure Protection," May 22, 1998. For an assessment of the wider bureaucratic response, see Birkland, *After Disaster*.
76. US Department of Justice, *Terrorism in the United States 1998*, 18.
77. Bendrath, Eriksson, and Giacomello, "From 'Cyberterrorism' to 'Cyberwar', Back and Forth," 66; and Bendrath, "The Cyberwar Debate".
78. Pentagon spokesman Kenneth H. Bacon, quoted in Gertz, "Eligible Receiver".
79. See Rid, *Rise of the Machines*.
80. See National Domestic Preparedness Office, *Blueprint for the National Domestic Preparedness Office*.
81. *Public Papers of the President, William Jefferson Clinton,* (2000), vol. 1, Remarks on the National Plan for Information Systems Protection and an Exchange with Reporters, January 7, 2000, 14.
82. See also Kessler, "A Cautionary Tale for Politicians"; Krugman, "Al Gore and the Internet"; and Markoff, "The Team That Put the Net in Orbit".
83. Lacey, "Clinton Gives a Final".

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

James D. Boys is an associate professor of International Political Studies at Richmond University in London. Between 2012 and 2015, he was a senior visiting research fellow at King's College, London. His writing and opinion has been featured in *The Guardian, The Daily Telegraph*, and *The Hill*. He is a regular commentator on a wide array of international media outlets, including *Sky News, CNBC, BBC World News, Aljazeera English, Bloomberg TV,* and the *BBC News Channel*. As a political historian, his work focuses on the relationship between foreign and domestic policy in the United States with a particular emphasis on the Clinton administration. His first book, *Clinton's Grand Strategy: US Foreign Policy in a Post-Cold War World* was published by Bloomsbury in 2015. His second book, *Hillary Rising,* was published by Biteback in 2015, establishing him as the only British academic to have published a political biography of Hillary Clinton. His third book, *Clinton's War on Terror: Redefining US Security Strategy 1993–2001*, was published by Lynne Rienner in 2018.

ORCID

James D. Boys http://orcid.org/0000-0002-1191-5762

Bibliography

Albright, Madeleine. *Madame Secretary*. New York: Miramax, 2003.

Armistead, Leigh, ed. *Information Warfare: Separating Hype from Reality*. Washington, DC: Potomac Books, 2007.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165.

Ayers, Robert. "The New Threat: Information Warfare." *The RUSI Journal* 144, no. 5 (1999): 23–27.

Birkland, Thomas A. *After Disaster: Agenda Setting, Public Policy, and Focusing Events*. Washington, DC: Georgetown University Press, 1997.

Bendrath, Ralf. "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." *Information and Security* 7 (2001): 80–103.

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. "From 'Cyberterrorism' to 'Cyberwar', Back and Forth: How the United States Securitized Cyberspace." In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello, 57–82. Abingdon: Routledge, 2007.

Boys, James D. *Clinton's Grand Strategy: US Foreign Policy in a Post-Cold War World*. London: Bloomsbury, 2015.

Broad, William J. "Computer Security Worries Military Experts." *New York Times*, September 25, 1982.

Cannon, Lou. *President Reagan: Role of a Lifetime*. New York: PublicAffairs, 1991.

Christopher, Warren. *Chances of a Lifetime*. New York: Scribner, 2001.

Clarke, Richard A. *Against All Enemies*. New York: Free Press, 2004.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: HarperCollins, 2010.

Clinton, Bill. *My Life*. New York: Knopf, 2004.

Conway, Maura. "Cyberterrorism: Hype and Reality." In *Information Warfare: Separating Hype from Reality*, edited by Leigh Armistead, 73–94. Washington, DC: Potomac Books, 2007.

Denning, Dorothy. "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives." (2000). Accessed July 23, 2017. http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf

Denning, Dorothy. "Cyberwarriors: Activists and Terrorists Turn to Cyberspace." *Harvard International Review* 23, no. 2 (2001): 70–75.

Devost, Matthew G., Brian K. Houghton, and Neal Allen Pollard. "Information Terrorism: Political Violence in the Information Age." *Terrorism and Political Violence* 9, no. 1 (1997): 72–83.

Doty, Roxanne Lynn. "Foreign Policy as Social Construction: A Post-Positive Analysis of US Counterinsurgency Policy in the Philippines." *International Studies Quarterly* 37, no. 3 (September 1993): 297–320.

Dumbrell, John. *Clinton's Foreign Policy: Between the Bushes 1992–2000*. London: Routledge, 2009.

Dunn Cavelty, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* Abingdon: Routledge, 2008.

Dunn Cavelty, Myriam. "Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology & Politics* 4, no. 1 (2007): 19–20.

Dunn, Myriam, and Isabelle Wigert. *The International CIIP Handbook 2004: An Inventory of Protection Policies in Fourteen Countries*. Zurich: Center for Security Studies, 2004.

Gates, Robert M. *From the Shadows: The Ultimate Insider's Story of Five Presidents*. New York: Simon & Schuster, 1996.

George, Jim. *Discourses of Global Politics: A Critical (re)introduction to International Relations*. Boulder, CO: Lynne Rienner, 1994.

Gertz, Bill. "Eligible Receiver." *Washington Times*, April 16, 1998.

Goldberg, Donald. "The National Guards." *OMNI Magazine*, May 1987, 44–46.

Gompert, David. "Keeping Information Warfare in Perspective." *RAND Research Review* 19 (Fall 1995). Available at http://web.archive.org/web/20000229153230/http://www.rand.org:80/publications/RRR/RRR.fall95.cyber/perspective.html

Gordon, Sarah, and Richard Ford. "Cyberterrorism?" *Computers & Security* 21, no. 7 (2002): 636–647.

Green, Joshua. "The Myth of Cyberterrorism." *Washington Monthly*, November 2002, 8–13.

Greenhouse, Linda. "Computer Security Shift is Approved by Senate." *New York Times*, December 24, 1987.

Hua, Jian, and Sanjay Bapna. "How Can We Deter Cyberterrorism?" *Information Security Journal: A Global Perspective* 21, no. 2 (2012): 102–114.

Hyland, William G. "A Mediocre Record." *Foreign Policy* 101 (Winter 1995–1996): 69–74.

Hyland, William G. *Clinton's World: Remaking American Foreign Policy*. Westport, CT: Praeger, 1999.

Jarvis, Lee, and Stuart Macdonald. "What is Cyberterrorism? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27, no. 4 (2015): 657–678.

Joint Security Commission. *Redefining Security: A Report to the Sectary of Defense and the Director of Central Intelligence.* Washington, DC: Joint Security Commission, February 28, 1994.

Kessler, Glenn. "A Cautionary Tale for Politicians: Al Gore and the 'Invention' of the Internet." *Washington Post*, November 4, 2013.

Krugman, Paul. "Al Gore and the Internet." *New York Times*, December 9, 2007.

Lacey, M. "Clinton Gives a Final Foreign Policy Speech." *New York Times*, December 9, 2000.

Lake, Anthony. *Six Nightmares*. Boston, MA: Little, Brown, 2000.

Laqueur, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press, 1999.

Lawson, Sean, and Michael K. Middleton. "Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991-2016." Paper presented at the Legal and Policy Dimensions of Cybersecurity conference, George Washington University, Washington, DC, September 27–29, 2016.
Mandelbaum, Michael. "Foreign Policy as Social Work." *Foreign Affairs* 75, no. 1 (January–February 1996): 16–32.
Markoff, John. "Blown to Bits; Cyberwarfare Breaks the Rules of Military Engagement." *New York Times*, October 17, 1999.
Markoff, John. "The Team That Put the Net in Orbit." *New York Times*, December 9, 2007.
Miller, Linda B. "The Clinton Years: Reinventing US Foreign Policy?." *International Affairs* 70 (October 1994): 621–634.
Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: RAND, 1996.
Muravchik, Joshua. "Carrying a Small Stick." *National Review* 2 (September 1996): 57–62.
National Academy of Sciences. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press, 1991.
National Domestic Preparedness Office. *Blueprint for the National Domestic Preparedness Office.* Accessed May 30, 2017. https://www.hsdl.org/?view&did=438600
National Security Strategy of the United States, 1995. Washington, DC: Government Printing Office, 1995.
National Security Strategy of the United States 1998. Washington, DC: Government Printing Office, 1998.
National Security Strategy of the United States 1999. Washington, DC: Government Printing Office, 1999.
Omand, Sir David, and Mark Phythian. "Ethics and Intelligence: A Debate." *International Journal of Intelligence and Counterintelligence* 26, no. 1 (2013): 38–63.
Pollitt, Mark M. "Cyberterrorism — Fact or Fancy?." *Computer Fraud & Security* 2 (February 1998): 8–10.
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, February 11, 1970.
Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Basingstoke: Palgrave Macmillan, 2014.
Rid, Thomas. *Rise of the Machines: A Cybernetic History*. New York: W.W. Norton & Company, 2016.
Sagan, Scott D. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, NJ: Princeton University Press, 1993.
Sale, Richard T. *Clinton's Secret Wars*. New York: St. Martin's Press, 2009.
Schwartau, Winn. "Fighting Terminal Terrorism." *Computerworld*, January 28, 1991.
Schwartau, Winn. *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. 2nd ed. New York: Thunder's Mouth Press, 1996.
Smith, George. "An Electronic Pearl Harbor? Not Likely." *Issues in Science and Technology* 15, no. 1 (Fall 1998): 68–73.
Soderberg, Nancy. *Superpower Myth*. New York: Wiley, 2005.
Tsui, Chin-Kuei. *Clinton, New Terrorism and the Origins of the War on Terror*. Abingdon, Oxon: Routledge, 2016.
Ullman, Richard H. "A Late Recovery." *Foreign Policy* 101 (Winter 1995–96): 75–79.
Warner, Michael. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, no. 5 (October 2012): 781–799.
Weimann, Gabriel. "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict & Terrorism* 28, no. 2 (2005): 129–149.
Weldes, Jutta. "Bureaucratic Politics: A Critical Constructivist Assessment." *Mershon International Studies Review* 42, no. 2 (November 1998): 216–225.
Wirtz, James J. "The Cyber Pearl Harbor." *Intelligence and National Security* 32, no. 6 (2017): 758–767.