

Critical Infrastructure Protection in Comparative Perspective

Kevin Quigley
School of Social and Political Studies
University of Edinburgh
kevin.quigley@ed.ac.uk

Abstract

This paper examines comparatively how the US and UK government interacted with industry to ensure stability of service across the critical infrastructure in the face of the challenges associated with the Year 2000 Computer Bug (Y2K). The paper is organised according to the categories of Marsh and Rhodes (1992) Policy Networks Typology and the data concerning Y2K come from official UK/US government sources, in-depth, semi-structured interviews and newspaper articles. The paper concludes that the US government relied more heavily on market mechanisms to motivate the owners of the critical infrastructure to combat the bug whereas the UK government opted for standardising the approach among a small but powerful group within industry. There were trade-offs implicit in both approaches. The paper ends with some lessons for present-day critical infrastructure protection (CIP).

Introduction

Critical Infrastructure Protection (CIP)¹ continues to climb the policy agendas for both the US government and the UK government, respectively, in light of recent high profile challenges to the successful operation of the infrastructure, such as the UK's petrol crisis in 2000, 9/11, the 2003 North/Eastern Power Failure, Hurricane Katrina and the July 7 underground bombings.² The Department of Homeland Security (DHS) marks perhaps the single most significant effort to join up both physical and cyber CIP operations. DHS represents the amalgamation of 22 formerly separate agencies. In 2005 President Bush requested \$27.2bn for DHS initiatives, which represents 57.4% of the US government's total budget for homeland security (GAO, 2005D, 8). This amalgamation has represented a massive undertaking, which has included significant growing pains and attracted many criticisms. (See for example GAO, 2005C).

One theme that recurs in GAO reports on homeland security initiatives is the (at times) awkward relationship that exists between the private sector and the government (GAO, 2001; GAO, 2002; GAO, 2005B; GAO, 2005D; GAO, 2005C). As 85% of the American critical infrastructure is owned and operated by the private sector, the relationship between it and the government is an essential component of CIP initiatives. In one recent study on cyber-security in particular, the GAO concluded that DHS has been especially ineffective. The GAO notes DHS's CIP initiatives suffer from the department's inability:

¹ GAO defines Critical Infrastructure Protection as "activities that enhance the physical and cyber-security of the public and private infrastructures that are critical to national security, national economic security, and national public health and safety" (GAO, 2005, 4).

² There are several recent government publications on the topic. See for GAO (2002), *Information-Sharing: Practices that Can Benefit Critical Infrastructure Protection* and GAO (2004), *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*.

to create effective partnerships with the private sector stakeholders; to facilitate information-sharing between interested parties; to provide ‘value-added’ in its function as the ‘hub’ for CIP information gathering and dissemination (GAO, 2005, 55-59).

This paper will use the case of the Year 2000 computer bug (Y2K)—an almost un-researched ‘cyber’ case study post January 1, 2000³— to examine comparatively two *different* models for CIP. Y2K represented a pervasive technological problem that occurred in a highly interdependent environment that straddled organisations in both the public and private sectors and posed a significant challenge to the successful operation of the critical infrastructure. Yet despite both governments ostensibly pursuing the same goal in the run-up to January 1, 2000, “stability across the infrastructure,” their approaches were notably different. The UK government adopted a model that might usefully be thought of as a *Corporatist* approach. It penetrated elite industry circles; it engaged directly with a relatively small but influential group of industry leaders and, to a degree, standardised the approach and reporting mechanisms among ‘key’ organisations. The US government, in contrast, opted for what might be described as a *Pluralist* approach. It engaged with a large number of organisations, none of which were deliberately prioritised. The US government also stayed at arms-length from industry throughout the Y2K process but rolled-back legal protections by way of increasing market pressures on all sectors to co-operate.

³ Despite the cost and magnitude of the Y2K projects, other than a few, brief government post mortems, there has been almost nothing published on the case post January 1, 2000.

While the governments may have *opted* for these different approaches to structure government/industry intermediation on Y2K issues, in fact, Rhodes argues that such conventional lenses do not accurately reflect the policy process. He argues Corporatism as an explanatory tool puts too much stress on the top-down nature of policy-making, on economic interests and on aggregate analysis, for instance (Rhodes, 1997, 32).

For Rhodes and others, 'networks' is a more useful way of explaining the policy-making process. Issue Networks exist somewhere between the selective and hierarchical arrangement of Corporatism and the flatter, more competitive nature of Pluralism. Networks assume multiple partnerships, complicated calculations and decreased predictability. While they assume some degree of stability or continuity over time, 'webs of influence,' rather than a powerful few, guide their progression (Hecl, 1978, 102-105).

This paper is organised according to the four dimensions of Marsh and Rhodes (1992) Issue Network⁴: *Membership, Integration, Resources* and *Power*. The Issue Networks approach will not be applied rigidly; however, it will be assumed that networks and these four organising concepts in particular do characterise the dynamics of policy-making. Hence, these conceptual lenses will be used to examine and compare the US government's Pluralist approach with the UK government's Corporatist approach with an eye to determining the impact each government had along the four dimensions of the Issue Network. The paper ends with observations about the two approaches and offers lessons for present-day CIP and government interactions with the private sector, in

particular. The data concerning Y2K is drawn from official UK/US government sources, over 60 in-depth, semi-structured interviews and an analysis of newspaper articles from both countries.

Y2K Recalled

Y2K, or the ‘millennium bug,’ referred to the fact that in computer programmes created in the 1950s and onwards most year entries had been identified in two-digit shorthand—1965, for instance, was entered as ‘65’. Initially this short hand was adopted to save on expensive computer memory. Through time it simply became standard practice. As the year 2000 approached, however, anxiety grew that systems would be unable to distinguish between twentieth century entries and twenty-first century entries (e.g., Would ‘01’ be treated as ‘1901’ or ‘2001’?). Such ambiguity, it was feared, would result in systems failing or producing inaccurate information. At the very least it made information unreliable.

From the early nineteen nineties (when the first popular article about Y2K appeared) to the late nineteen nineties, the date-related computer glitch rose from relative obscurity to regular headline news. Between 1997 and 2000, for instance, three major newspapers from each of the two countries ran collectively over 800 articles on Y2K. In 1997—and prior to any significant government executive intervention in the economy—the tone of

⁴ Marsh and Rhodes (1992) describe five types of Policy Networks along a continuum: Policy Communities/Territorial Communities, Professionalised Networks, Intergovernmental Networks, Producer Networks and Issue Networks

the media coverage was overwhelmingly alarming (Quigley, 2005). 1997 estimates of the world-wide cost of fixing Y2K-related problems ranged from \$300bn to \$1 trillion⁵.

The Congress and the GAO were particularly aggressive in seeking-out information about Y2K. IT consultants and Y2K specialists appeared before congressional committees frequently to testify about the potential consequences of the bug. Between 1996 and 1999 congressional committees and subcommittees held over 100 hearings on the subject and the GAO issued 160 Y2K reports and testimonials. Bruce Hall from Gartner testified to a congressional committee: ‘we must accept that risk exists in *any* technology that was ever programmed by a human, examine such technology for possible failures, and form remediation strategies’ (Hall, 1997; original emphasis). Gartner advised ‘plan not to finish’ and advocated ‘active prioritisation and technology triage.’ Gartner predicted that 50% of organisations would not finish their Y2K plans. Ann Couffou, Managing Director at Giga Year 2000 Relevance Service, testified to Congress in 1997: ‘anything with an electronic component should be suspect. The rule should be *guilty until proven innocent*’ (Coffou, 1997; original emphasis). She noted the following systems were susceptible to Y2K-related failures⁶: manufacturing control systems; elevators; telephone systems; medical equipment; stock markets; military messaging systems; radioactive material waste systems; fax machines, electronic time clocks; landscaping systems; vending machines; thermostats; and micro-wave ovens.

⁵ By the year 2000, the US Treasury estimated the cost to be \$300bn world-wide.

⁶ Couffou was discussing the vulnerability of embedded systems. Embedded systems contain programmed instructions running via processor chips. The processor chips are similar to standalone computers buried inside various kinds of equipment

In the UK the bug received less attention in parliament. The NAO published seven reports and the Public Accounts Committee held three hearings on Y2K but they were no less alarming. A report by the British House of Commons summarised the more pessimistic interpretation of the outcome this way:

The most 'doom and gloom' predictions foresee: planes tumbling from the sky, governments falling as national stability is threatened, runs on cash forcing banks to close as people anticipate problems with their accounts, all automatic doors refusing to open, industrially machinery automatically shutting down, no electricity or water supply and traffic lights going out of sequence causing crashes. In the event of such calamity, the UK will be relying on its contingency planning to save the day (House of Commons Library, 1998).

Much like the threat of terrorism today, for instance, Y2K was described as a pervasive and imminent threat that could undermine the successful operation of the infrastructure, and indeed, society as a whole. In 1998, with a high degree of uncertainty, considerable interdependence across organisations and sectors and few formal or informal means by which one could obtain reliable information about the Y2K-related status of organisations deemed critical to the infrastructure both governments intervened. The UK government created the National Infrastructure Forum (UK/NIF) and the US government created sector-level Y2K Working Groups (US/WG). The remainder of the paper examines comparatively the effectiveness of these two fora, and is organised according to the concepts of an Issue Network, starting with who was included in the formal Y2K preparations, and who was not.

Membership

Membership of Issue Networks is large and encompasses a range of affected interests (Marsh and Rhodes, 1992, 251). And so it was with Y2K. As the NAO noted, 'there are

very few areas of modern life that are not touched by information technology. The millennium threat [was] a business wide problem that affect[ed] everyone' (NAO, November 1999). The complex and interdependent nature of supply chains and the pervasive nature of technology meant that the potential for problems were numerous, and indeed, potentially incomprehensible. In the face of such a dynamic both governments selected specific sectors to include in their Y2K initiatives. (See Table 1 below.)

Tranche (UK-only)	National Infrastructure Forum (UK/NIF): 25 Sectors		Working Groups (US/WG): 26 Groups
1	Electricity		Benefits Payments
	Gas		Building and Housing
	Fuel Supplies		Consumer Affairs
	Telecommunications		Defence and International Security
	Water and Sewerage		Education
	Financial Services		Emergency Services
2	Essential Food and Groceries		Employment-Related Protections
	Rail Transport		Energy (Electric Power)
	Air Transport		Energy (Oil and Gas)
	Road Transport (Local Government)		Financial Services
	Sea Transport		Food Supply
	Hospitals and Health Care		Health Care
	Fire Service		Human Services
	Police		Information Technology
	Broadcasting		International Relations
	Local Government		International Trade
	3	Sea Rescue	
Weather Forecasting			Police and Public Safety
Post and Parcels			Small Business
Welfare Payments			State and Local Government
Flood Defence			Telecommunications
Criminal Justice			Transportation
Tax Collection			Tribal Government
Bus Transport			Waste Management
Newspapers			Water Utilities
			Workforce Issues

Table 1: Critical Sectors in the US and UK

On the whole, Table 1 shows that labelling is slightly different but the entries are similar. In some cases US/WGs subsumed many of the functions that the UK/NIF sectors treated separately. For example, the US/WG Transportation included five UK/NIF categories. While the lists in Table 1 are similar, they are by no means identical. Some entries reflect arrangements that existed in one country but not in the other (e.g., state government⁷). The US list seems also to be somewhat broader in scope: the US includes Education, for instance, whereas the UK list appears to be akin to a conventional engineering view of the infrastructure⁸. There are other similar omissions. For instance, the US Government included Defence and International Relations among the Working Groups, whereas the UK government decided not to include the Ministry of Defence (MOD) nor the Foreign Office in the UK/NIF explicitly, despite both having sizeable Y2K operations⁹. The UK's omission of the IT sector, in particular, is ironic. One commonly held view in the IT community that explains why the Y2K problem had been neglected in the early to mid-nineties is that IT did not have a sufficiently high profile at the executive level in most organisations. Despite this problematic legacy, the UK government still chose to see IT as a function that supported critical sectors much like Small- to Medium-sized Enterprises (SMEs, also omitted from the UK/NIF), rather than as a sufficiently critical sector in its own right, such as gas or electricity.

⁷ Devolution in the UK occurred in the late stages of Y2K planning and had little impact on Y2K plans. See for example NAO, 1999C and NAO 1999D.

⁸ In Lee Clarke's *Worst Cases*, he notes that schools are an important part of the infrastructure but are frequently ignored in present-day US CIP initiatives (2006, 165-66; 170-171).

⁹ The MOD, for example, accounted for 39 per cent of the UK Government's overall Y2K expenditures (Cm 4703, 2000, 76).

Membership in the US/WGs was made-up of government departments and related industry associations. The industry associations typically represented massive memberships—frequently in the thousands; membership within the industry associations were multiple and voluntary. The US government did not afford individual organisations a special status within the US/WGs. Membership in the UK/NIF, in contrast, included government regulators and usually a handful of the top service providers from the respective sectors. Although membership was not strictly compulsory, there was considerable pressure for each major service provider to participate in the UK/NIF. It was a non-competitive arrangement in which the selected members were taken to represent their sectors. The table below illustrates the differences in membership between the two arrangements.

	No. of US/WG Organisations (<i>via trade associations</i>)	No. of UK/NIF Organisations (<i>via direct membership</i>)
Electric Power	3,000	*18
Oil and Gas	1,250	**47
Water	4,000	***26
Food Suppliers	55% of independent operators	36

Table 2: Organisations in Y2K CIP Initiatives

*England and Wales only. It includes generation, transmission and distribution. In addition, the UK/NIF included the electricity sector supplier as a whole

**This example does not include Northern Ireland entry

***England and Wales only

Source: Action 2000, 1999; President’s Council on Year 2000 Conversion, 2000

What we see emerging from the outset of both governments’ respective Y2K operations is characteristic of traditional Corporatist (UK/NIF) and Pluralist (US/WG) approaches (Schmitter, 1979; Vogel, 1986). There are several reasons that might explain the governments’ divergence. First, the UK government may have selected a Corporatist approach because they could do: it’s a smaller country geographically, which often has

fewer companies occupying a large percentage of the market in each of the sectors. Both options may equally be rooted in their histories, national routines or culture. For the purposes of this paper, however, we will remain agnostic about the reason for each government adopting its selected approach. Accepting the approach, we will look at the governments' abilities to integrate the network, facilitate resource exchange and consider the role 'power' played in ensuring Y2K compliance across the infrastructure.

Integration

In an Issue Network contacts fluctuate in frequency and intensity, and agreement is tenuous (Rhodes, 1997, 44). The Corporatist approach to the UK/NIF managed the tenuous nature of such integration by limiting the membership to a small, agreeable group; the US/WG sought to manage the tenuous nature of the group by *not* seeking agreement.

Part of the purpose of the UK/NIF and US/WG, respectively, was to facilitate information-sharing within and across sectors. They started, first, by building on pre-existing institutional arrangements, such as the industry association in the US and the regulators in the UK. Information was collected, summarised and made public, at the sector level. The sector level reporting, therefore, created some degree of cross-sector disclosure.

The US government's pluralist approach was more inclusive but less cohesive. US/WGs were established to facilitate information-sharing (e.g., best practices) but the terms of

compliance were not dictated to participating organisations, by either the industry association or the government department. President Clinton's Y2K Executive Order (13073) directed the government to work *with* industry on Y2K issues but not direct it—it was up to industry to sort its own problems out. The US government believed that there were strong enough market signals to move organisations towards compliance (President's Council, 2000). Nor did the US government readily discriminate in its interactions with industry. As noted, the US/WGs engaged with thousands of organisations that contributed to the successful delivery of critical infrastructure services, albeit indirectly *via* trade and industry associations. (See Figure 1.)

The UK government's approach, in contrast, was more interventionist and joined-up but also more selective. The UK/NIF represented a small sample of organisations from each sector whose actions were much easier to co-ordinate and for whom the UK/NIF created a degree of group pressure to comply. The total membership in the UK/NIF counted in the hundreds, not the thousands. In this context, the UK government was able to enforce common standards¹⁰ and a mandatory third party audit among all participating members. While SMEs and the IT industry were not in fact a recognisable sector in the UK/NIF, it was understood as part of the standard UK/NIF approach that members would ensure their supply chains were compliant. (See Figure 2.)

¹⁰ UK/NIF assessments included, at a minimum, IT systems; embedded chips; infrastructure; supply chain; behaviour patterns; business continuity plans; and millennium operating regimes, which were plans that dealt specifically with the days leading up to January 1, 2000 (Action 2000, 1999, 6).

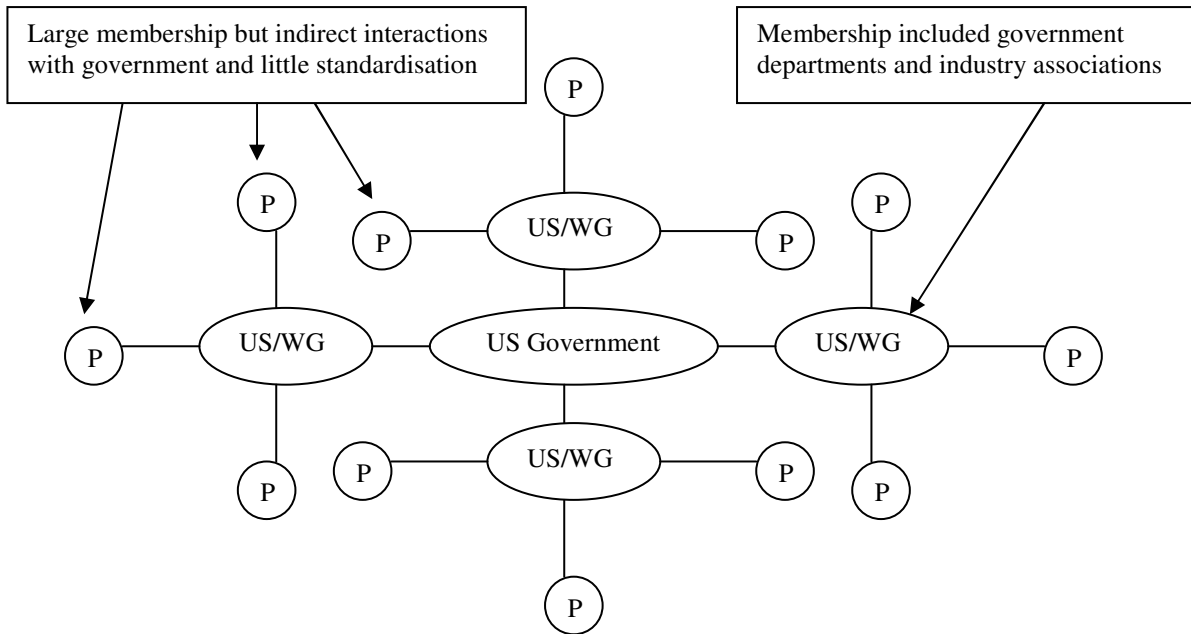


Figure 1: US/WG Model (where *P* is an industry participant)

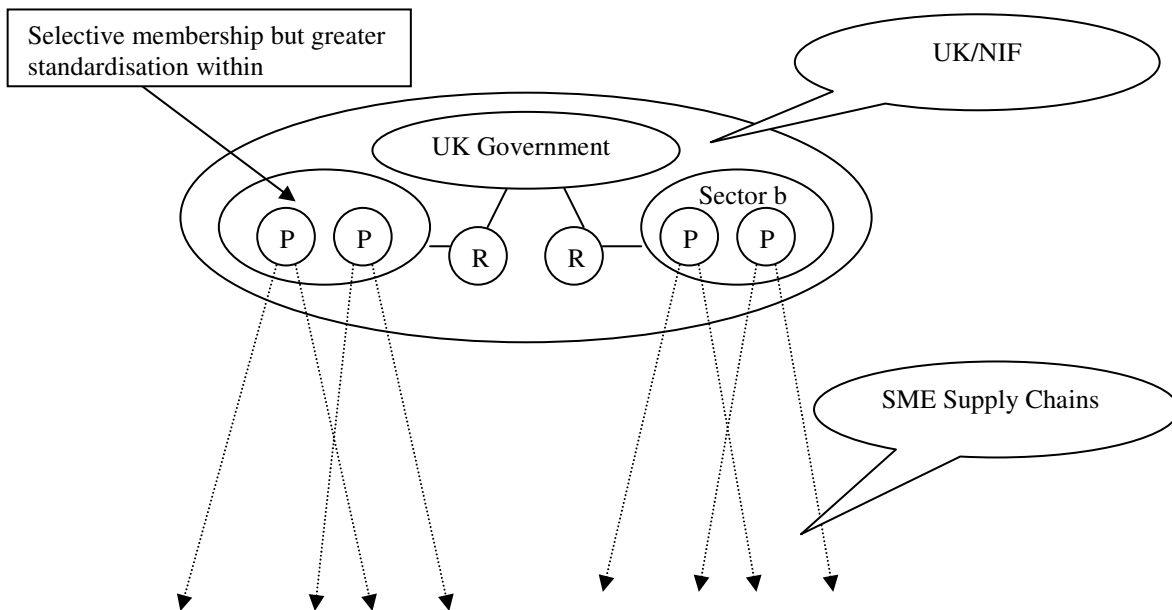


Figure 2: UK/NIF Model (where *R* is the regulator and *P* is an industry participant)

Whereas the Corporatist approach had a relatively narrow catchment, the Pluralist approach was potentially futile in its (in)ability to integrate such a large and tenuous membership. Aviation provides a good illustration. The UK/NIF (initially) included 15 aviation service providers. In fact, the CAA regulates five different sub-sectors¹¹ that include over 1,800 organisations, from which the CAA tried to secure Y2K-compliant guarantees. The 1,800 organisations vary in size and impact in the supply chain. Some are domestic but many are not, which made it difficult at times to obtain reliable information. There were some foreign-based companies for instance that never replied to CAA Y2K information requests. Ultimately there were about 20 of the 1,800 CAA-regulated organisations (i.e., a little over one percent) whose Y2K status was forever unknown. The UK/NIF membership was a *practical* way forward. It allowed the government to declare the industry as compliant, when in fact it was just referring to a specific definition of compliance, which focussed exclusively on (initially) the top 15 service providers.

The FAA had similar problems, but found different solutions. During interviews, staff indicated that a senior senator from the Special Committee on the Year 2000 Technology Problem Senate's directed the FAA to revoke the licenses of any certified organisation that failed to produce a Y2K compliance certificate. FAA staff resisted the directive strongly. They argued it was impossible to contact 'every mom and pop shop' licensed to fly a plane in the US. There were too many, several of which were remote and in any

case seasonal (*i.e.*, summer only) operations. Even if one could send them all a letter, one could not guarantee a reply, let alone an audit. In any event, without any concrete evidence of pending systems failure (after all, it was impossible to say for sure which systems, if any, would fail), the FAA could not revoke organisations' licences.

Eventually, the senior Senator and the congressional committee retracted the request and accepted the FAA's proposal—that the FAA would send a letter to each organisation with a license and would try to secure as many replies as possible. Otherwise, the FAA confined itself to organising 'Industry Days' in which participating organisations shared information voluntarily about their Y2K status.

Resource Dependency

In an Issue Network, the basic relationship is consultative and the capacity to regulate individual members varies (Rhodes, 1997, 44). In both the US and the UK reliable Y2K information was often a difficult resource to obtain: the limited resources and time available and the legal context in the US combined to create a simultaneously needy yet cautious market in the face of the crisis. In the US, the Pluralistic approach led to a feeling of isolation for many; in the UK, the Corporatist approach was more joined-up but arguably was even less transparent than the atomistic approach in the US.

We will start with the limited time and resources. In 1997 there was considerable anxiety that neither the US nor the UK economies had sufficient human resources to fix the myriad technologies in the relatively short time available. At the outset the perceived

¹¹ Air Operator; Maintenance; Aerodromes; Air Traffic; and Design and Production. For a fuller account of the CAA's management of Y2K, see Quigley, 2005B.

shortage of qualified programmers, and especially of older computer languages such as COBOL, led a House of Commons Standing Committee to note that programmers' salaries had increased anywhere from two- to four-times their pre-Y2K salaries (Standing Committee on Science and Technology, Chapter 5, page 3). Some organisations were particularly vulnerable because they had out-sourced much of their IT staff and intelligence, and were therefore entirely dependent on external organisations for their Y2K plans.

Again, we see a selective intervention by the UK government. In March 1998 Prime Minister Blair announced a special initiative to give would-be programmers a quick lesson in applying Y2K-related fixes. While the government anticipated that the so-called 'bug-busters' program would be popular, ultimately the take-up was poor and the program was considered a flop (Jones, 1998).

Organisations in both the US and the UK were more responsive than pessimists had anticipated. First, many larger organisations with large IT budgets and long-term IT strategies had sizeable Y2K operations in place from about 1996. For those organisations that started later than 1996, they began prioritising Y2K work, delaying other IT tasks and sharing resources within organisations (NAO, 1999, 35). Many appointed a Y2K lead to the executive who was supported by a Y2K office. These offices established standards and timelines and gathered information from within their organisations as well as from among their key suppliers. But perhaps most importantly, although many organisations had very poorly documented inventories initially, once the inventory was

taken and some testing had occurred, IT staff started to feel that their systems were not as vulnerable as they had initially been led to believe. Many systems, for instance, did not have any date functionality at all, or else the date-function was not critical to the successful operation of the system.

Other anxieties were also dispelled. Despite claims that programmers could ‘name their price’ for Y2K related work, for instance, most organisations learned that existing IT resources could manage the additional workload—with the help of some overtime pay (Taylor, 1999). As was noted by interview subjects, it is very difficult to bring in new people on short notice to work on a project that requires the knowledge of one’s entire business as well as all the systems that underpin it.

But just because they were making more progress than anticipated, that does not mean they were sharing this information across sectors or even organisations. The legal context constrained information-sharing in the US in particular. There were numerous legal barriers and financial disincentive that prevented the free exchange of Y2K-related information across organisations. First, if organisations offered information about Y2K that turned out to be incorrect—either Y2K advice to their supply chain or a report of their own Y2K status to external stakeholders—they could be held liable for any losses that resulted. Second, disclosure of their Y2K status could damage their share value—whether they were spending a lot on Y2K (‘they must be vulnerable’) or a little (‘they’re not spending enough’). Interview subjects from Congress noted this latter problem in particular effected their ability to secure witnesses for congressional committees. In

short, there was very little incentive for industry leaders to say anything—good or bad—about their Y2K status.

By way of reply to this problem, the US government enacted Y2K legislation. The legislation dictated that if an organisation offered advice in good faith that turned out to be incorrect, it could not be held accountable. Moreover, if one's systems failed, then the IT provider had 90 days to fix the system, during which time the owner had little legal recourse to recover expenses or compensation for lost revenue, for instance. The legislation also capped punitive damages. The purpose of the legislation was to force organisations to become proactive in their Y2K plans—start talking to their supply chains, sharing information and fixing problems, rather than waiting for failures or pursuing suppliers in slow, costly legal pursuits. The New York Times argued the legislation suspended people's right to sue (New York Times Editorial Desk 1999A; 1999B).

After the legislation was passed into law, several large organisations, such as those in the telecommunications sector, started sharing information with smaller companies and suppliers. The Federal Aviation Administration (FAA) with the co-operation of IATA, the aviation industry association, started sponsoring 'Industry Days' (noted above) in which all critical sectors shared information about their Y2K progress (Quigley, 2005B). Similarly, leaders of the electric power industry began a series of regional conferences for local distribution companies in which they discussed problems, particularly with

embedded chips, as well as testing protocols and contingency planning (President's Council on Year 2000 Conversion, 2000, 6).

The legal context in the UK was less confining than that which was in the US prior to its Y2K legislation. In testimony to the UK House of Commons Science and Technology Committee, Barclays Bank noted, "relying on legal remedies to address the problem is illusory" (3.7). The cost of Y2K-compliance was seen as less than the benefits. And the risks associated with waiting until one's systems failed were considered too high. First, in the event of a large systems failure, one's business could go bankrupt long before a court decision. Second, if particular businesses were pursued in court by numerous claimants then the businesses would likely go bankrupt, and as a result no or few organisations would be compensated (3.7). Instead, CCTA (the government's IT agency) and the House of Commons Standing Committee on Science and Technology recommended that organisations move quickly to arbitration in the event of legal disputes (CCTA, 1997, 35-36; Standing Committee on Science and Technology, Recommendations, page 2).

Again the UK government went further than the US. By way of making the process of information exchange more accessible to the public and other sectors, the UK/NIF gave each sector a 'traffic light' grading. There were three possible assessments: red (in danger of material disruption), yellow (some risk but agreed containment plan) and blue (no identified risk). Ostensibly, the intention of the traffic light system was to create a standard by which all sectors could be judged and compared. Most sectors ran behind

schedule but ultimately achieved a 'blue light' from the UK/NIF before January 1. The Figure below summarises the results.

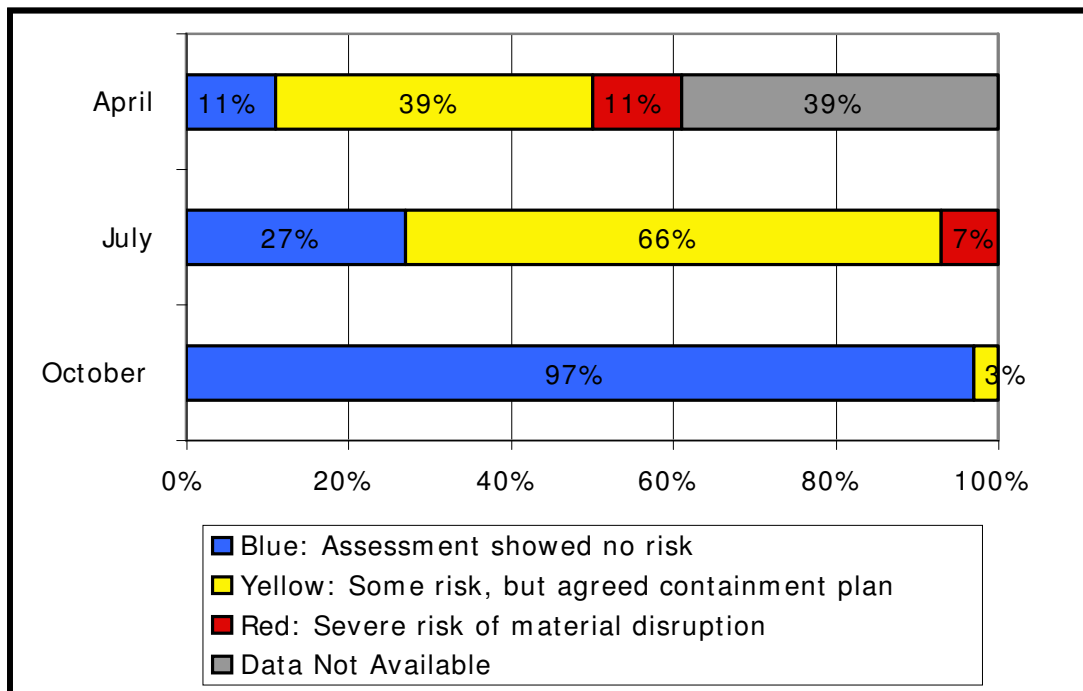


Figure 3: UK/NIF: Subsector Progress towards Y2K Compliance, 1999

Note: The 25 sectors were subdivided into 61 subsectors. Any subsectors showing any degree of ‘red’ were placed in the red category. Subsectors showing no red but at least some yellow were placed in the yellow category. Only those subsectors that were graded with a 100 per cent blue rating are captured under blue.

The reporting mechanism was ambitious but in fact there were a number of limitations.

First, the government deliberately selected ‘blue’ instead of ‘green’ because the Government was uneasy about declaring definitively that any sector would not experience disruption. Second, while the audits standardised the approach across the sectors at a high level, the specifics of the audits—who the auditor would be and what would constitute Y2K compliance—was a negotiated process between the sector-specific regulator and the UK/NIF participants. This negotiation always remained at the sector level and therefore the extent to which it was truly standardised across sectors is questionable. Third, UK/NIF was voluntary and therefore tenuous. For instance, one organisation from the aviation sector dropped out of the UK/NIF because it could not meet the UK/NIF timelines. Yet the government still reported the sector as being Y2K

compliant when the time came. It simply stopped counting 15 organisations and started counting 14 (Action 2000, 1999).

Power

For Issue Networks there is an unequal distribution of power, which reflects unequal resources and unequal access (Rhodes, 1997, 44). Rhodes's concept of power-dependence underpins Networks; the concept considers inter-organisational dependency, how the 'the rules of the game' are determined and how discretion is used in interpreting those rules. We will take each of the three in turn, and determine who was depending on whom, who benefited from the rules and who was afforded discretion.

Organisational Dependency

In the run-up to Y2K, organisations were assumed to be highly dependent on (complex) technology and organisationally interdependent. 'Probabilistic thinking'—the likelihood of an event occurring—changed to what Lee Clarke (2006) calls 'possibilistic thinking,'—imagining what *could* happen in a given context (Clarke, 2006, 5-6). The GAO (1999) summarised the threat of Y2K thus:

Our nation's reliance on the complex [sic] array of public and private enterprises having scores of systems interdependencies at all levels accentuates the potential repercussions a single failure could cause.

Yet despite this fragile arrangement, the US government played a comparatively *un-*intrusive role with respect to industry. The Congress brought attention to the issue and

the Executive enforced high standards among its own departments and agencies. But the US government's approach with industry was not to challenge established institutional arrangements. Instead, it withdrew: Y2K legislation *deregulated* the environment (i.e., it removed the rule of law) and in so doing created a setting in which operators were simultaneously on their own to ensure their own operation, and yet highly dependent on their supply chains, without legal recourse in the event of failure. This decision by government was not a neutral one, however. It meant those with existing power and influence in industry would continue to have it.

The UK government tried a more formal and interventionist approach to understanding the relationships across the infrastructure than the US government did. The Cabinet Office contracted Ernst and Young to conceptualise and map the relationship between sectors at a macro-level, which resulted in the sectors being prioritised by tranches (Action 2000, 1999, 4; Ernst and Young, 1998; tranches noted in Table 1). The sectors with the highest level of dependency on them were placed in Tranche 1. Tranche 1 had to report its Y2K status first to the UK/NIF, with Tranche 2 to follow a few weeks later, and so on (Action 2000, 1999, 4). An organisation in Tranche 2 could *not* claim to be Y2K compliant until all organisations in Tranche 1 had already demonstrated that they were compliant.

The project was ambitious (and unique in the world, in fact) but employed a rather limited method to understanding the situation. The Ernst and Young Y2K report (the blueprint for the UK/NIF approach to Y2K) was commissioned on a short and fixed

deadline. The report concedes at the outset: representatives from only a small sample of organisations were interviewed (sometimes as little as one person per sector); conclusions about process dependencies were based largely on the opinions of these individuals; and differing views emerged during the interview process (Ernst and Young, 1998, 3). Moreover, Ernst and Young conducted the research when arguably anxiety was at its peak (May 4, 1998, to June 30, 1998) (7)¹², an environment ripe for exaggerated claims.

In fact, the relationship between the tranches is more complex and interactive than the top-down flow chart would suggest. Tranche 2 includes the entire transport sector, for instance. It is easy to imagine services in Tranche 1 failing if human resources, goods and services are unable to be transported.

The UK/NIF clearly had a pro-business bias. The UK/NIF included mainly large corporations¹³. The UK/NIF failed to identify explicitly the role of potentially important social institutions, such as schools (unlike the US/WG), which are (arguably) not only a critical part of the infrastructure but could also play an important role during a crisis in the infrastructure. Similarly, 'welfare payments' is part of tranche 3. Yet it is questionable why, one, welfare payments was not grouped with financial services (whose membership was dominated by banks and assurances companies) and, two, financial services was considered tranche 1, compared to welfare payments being ranked as tranche 3. It seemed to suggest, as a member of a parliamentary committee commented,

¹² It might be argued that anxiety was at its peak because most organisations were behind in the assigned task, media coverage was intense and mostly negative and qualified human resources were perceived as scarce. One year later most of the anxiety had subsided. (See Quigley, 2005A.)

that the movement of some people's money is more important than that of others (Committee on Public Accounts, 1999).

There was also a London bias that made its impact felt in the rest of the UK. The south of England, for instance, occasionally experiences flooding, its homes frequently depend on gas lines and the train network is complex. Ernst and Young identify all these processes as 'key.' Yet, none of these problems exist (for all intents and purposes) in Northern Ireland, for example. Nevertheless, the government pressed each region to follow this same checklist. Hence, Northern Ireland was forced to divert resources to investigate issues that were highly unlikely to materialise¹⁴.

Those organisations with existing resources were able to build-up redundancies in order to avoid organisational failures caused by external failures. The Electricity Sector, for instance, included in all of its audits 'Communications' systems, which are critical to the successful operation of the power grid. In other words, 'telecommunications,' at least in so far as the electricity sector relies on it, would not be left for the telecommunications sector alone to manage. Of course this is also a measure of common sense: sectors were not left entirely to their own devices to fix Y2K problems that affected so many other sectors.

¹³ There were some exceptions. In food supply, for instance, the government included some small operators that provided food for remote areas.

¹⁴ Northern Ireland eventually distanced itself from the UK/NIF, established its own NI/NIF, and worked predominantly in that forum.

But it was usually not the status of the big operators that caused concern; they *had* the resources to deal with Y2K-related problems. Rather, large organisations were concerned about the status *smaller* businesses in the supply chain. The National Federation of Independent Business in the US warned: ‘330,000 firms risk closing their doors until the problem is fixed and more than 370,000 others could be temporarily crippled’ (US Special Committee, 1999, 128).

It was assumed for instance that the supply chains were all (critically) dependent on technology. In fact this was not consistently so. For instance, despite being the largest business group with 84 per cent of employee organisations, micro-businesses¹⁵ in the UK were found to be low risk: a full one-third of all micro-businesses did not even own a computer. Of those that did, most were eventually understood to be isolated, not interdependent. The state of play among SMEs varied depending on the sector. In the finance sector, for example, all were considered exposed to Y2K-related risks, but the perceived risks declined in other sectors. In transport and logistics sector 19 per cent did not have IT or process equipment, and in travel and restaurants, 27 per cent did not (Action 2000, 1999). And of course these figures do not reflect how critical the technology is to the successful operation of the organisation; nor does it acknowledge people’s capacity to respond creatively and/or competently to systems failures.

As the President’s advisor on Y2K, John Koskinen, concluded, the lack of information about what small businesses were doing was an on-going challenge that was never fully

¹⁵ fewer than ten employees

understood (President's Council on Year 2000 Conversion, 2000, 18). This uncertainty led to a call for high standards, across the board.

Rules of the Game

As the potential costs mounted, the insurance industry in both countries, normally the buffer against such risks, drafted exclusion clauses into policies to protect themselves from liability (Adams, 1997A). The Association of British Insurers, for instance, argued that Y2K was a foreseeable and preventable problem and was therefore not an insurable risk. ABI warned companies publicly that they could not expect to be covered for Y2K-related problems and that the onus was on policyholders to take preventative action.

With the insurance industry limiting its exposure, the IT industry became vulnerable to sizeable lawsuits, which prompted the Information Technology Association of America to argue for the Y2K legislation in the US. Yet ITAA was not alone in supporting the legislation. Eighty large companies and trade organisations also supported the legislation, including the National Association of Manufacturers and the US Chamber of Commerce (Simons, 1999). The larger organisations wanted to help key suppliers ensure their operations were Y2K compliant. But they also wanted to enforce standards along the supply chain. These larger organisations often pressured their supply chains to conduct audits. Some smaller organisations had no choice but to incur these costs even if they felt that they did not have any (or few) Y2K vulnerabilities or they simply had a

greater appetite for risk-taking. A number of US banks forced companies to undergo audits before they could receive loans while the Securities Exchange Commission (SEC) fined public companies that failed to disclose Y2K preparations by the SEC deadlines (Taylor, 1998)¹⁶. One IT executive from an SME noted ‘feeling forced’ by his primary customer into agreeing to an expensive Y2K audit that cost \$750 K¹⁷.

Definitions of Y2K compliance were usually quite specific. Again, the UK formally standardised the approach.¹⁸ This formal definition, as well as most Y2K compliance audit processes in both the US and the UK, frequently took a very narrow view of what ‘Y2K compliance’ was. In some respects, it had to be. It was peculiar yet specific problem; no one was prepared to say for certain that a system would not experience failure unless the exhaustive, standardised steps had been followed. It often dismissed short-cuts and work-arounds, which are common in the world of programming generally and had often been used with success with Y2K problems in particular.¹⁹

¹⁶ The SEC also had the right to revoke trading licenses if organisations continued to fail to meet Y2K disclosure standards.

¹⁷ This was an informal discussion I had with an individual. It was not formally documented.

¹⁸ In response to demand from the public sector, UK industry, and commerce in particular, the British Standards Institution committee developed a four-rule definition of Y2K compliance Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the year 2000. In particular: (1) No value for current date will cause any interruption in operation; (2) Date-based functionality must behave consistently for dates prior to, during and after year 2000; (3) In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules. (4) Year 2000 must be recognised as a leap year.

¹⁹ They did not accept, for example, a ‘windowing’ technique which allows programmers to apply *one* rule to programmes to cut back on the time required to fix every line of code. In brief, ‘windowing’ meant that programmers could pick a cut-off year—say 2029—and programme an instruction that interpreted any year entry that was ‘29 or lower’ as the twenty first century and any year entry that was ‘30 or higher’ as the twentieth century. One prominent Y2K consulting firm described ‘windowing’ as allowing the computer to ‘guess’ which century users meant when they entered data. In fact, windowing is a common practice in programming in general and was often used with success when dealing with Y2K.

The organisations that could enforce standards *across* sectors and organisations, such as Y2K auditors and consultants, satisfied a gap in the market. Compliance operations typically included five steps: inventory of systems, fix (when necessary), test (including all internal and external systems interfaces), conduct a third party audit and then develop contingency plans.

The high standards allowed some entrepreneurs to game the system. Some interview subjects claimed that IT service providers were deliberately evasive about the reliability of existing systems as a sales pitch for the new 'Y2K compliant' version of their product. Organisations that had out-sourced their IT operations were particularly vulnerable because they became entirely dependent on external organisations for their Y2K plans. The anxiety over Y2K resulted in short-term increased demand for new hardware and software. Some large organisations capitalised on the situation by creating 'software factories' that specialised in making clients' software Y2K-compliant. IBM, Cap Gemini and Unisys, for instance, had 23, 21 and 10 of such factories, respectively (Nairn, 1998).

By 1999 no large or even medium-sized organisations stood completely outside of Y2K-related scrutiny; all were expected to conduct and disclose some degree of Y2K-related preparedness, in both countries. The UK government was better able to penetrate industry to enforce those standards. However, once the UK government penetrated industry circles to enforce common standards, it effectively became a partner rather than an overseer in Y2K compliance, which pressured it to make deals with UK/NIF participants.

Discretion

Despite this seemingly exhaustive and detailed approach such a large and complex process necessarily had many built-in loopholes, which served largely major corporations but also exposed the difficulty in controlling such a sprawling and complex supply chains. Corporate plans that made Y2K-readiness statements were frequently vague. Larger organisations tried to impress by declaring how much they spent on Y2K, for instance.²⁰ In fact Y2K costs were not always reported consistently. The real cost of Y2K was the cost of *accelerating* purchase of goods or services to prevent Y2K-related losses. But often costs of replacing complete IT software and hardware were reported as Y2K costs. Y2K projects were often generously funded and therefore many included pet IT projects under the Y2K umbrella in order to secure funding. In short, bottom-line costs are at best highly dubious. Y2K auditors audited organisations' Y2K processes only. Auditing the technical work would have been too costly, slow and complex. Moreover, rarely would an outside firm of auditors know the systems better than the staff that worked on the systems on a regular basis—be they external contractors or internal IT staff. The audits served to reassure but rarely came up with many detailed criticisms. And as noted, given the number of trading partners there was always considerable anxiety about the vulnerability of systems and the readiness of SMEs and international trading

²⁰ The nine Wall Street firms that claimed to spend the most on Y2K, for example, reported that they spent \$2.8bn collectively (Smith and Buckman, 1999).

partners. The readiness of these key links in the supply chain were never fully understood or appreciated.

As noted, the US government's Pluralist approach depended almost exclusively on information it received from industry associations. One might think that this relationship was built on trust, but in fact it was more likely the opposite. Industry did not want government dictating the terms of compliance or interfering with their Y2K operations. Instead, both industry and government depended on the power of an unregulated market to pressure organisations towards compliance. In theory, SMEs could take or leave Y2K compliance. In fact, Y2K legislation left SMEs little comfort. They were on their own if their systems failed, and in any event, were likely bullied by bigger suppliers to adhere to their standards or an anxious customer base.

That the government was always at arms-length to industry, however, meant that there was also a clearer division between government and industry. This distance allowed the US government to provide assessments that were perhaps more impartial: not all organisations were considered compliant but most were, and US government reports reflect this uncertainty in a more transparent manner than their UK counterparts. (See for example President's Council on Year 2000 Conversion, 1999),

In contrast, the Corporatist approach in the UK undermined some of the goals the government was trying to achieve. The UK government penetrated and pressured industry to move towards compliance but in so doing compromised its position as an

arbiter of industry Y2K plans. In the UK compliance was as uncertain as in the US but the UK/NIF was less forthcoming about the uncertainty. Ostensibly, the intention of the traffic light system was to create a standard by which all sectors could be judged and compared. In fact there were a number of limitations to the reporting mechanism. First, the government deliberately selected 'blue' instead of 'green' because the Government was uneasy about declaring definitively that any sector would not experience disruption (Cite NAO). Second, while the audits standardised the approach across the sectors at a high level, the specifics of the audits—who the auditor would be and what would constitute Y2K compliance—was a negotiated process between the sector-specific regulator and the UK/NIF participants. This negotiation always remained at the sector level and therefore the extent to which it was truly standardised across sectors is questionable. Third, UK/NIF was voluntary and therefore tenuous. For instance, one organisation from the aviation sector dropped out of the UK/NIF because it could not meet the UK/NIF timelines. Yet the government still reported the sector as being Y2K compliant when the time came. It simply stopped counting 15 organisations and started counting 14 (Action 2000, 1999).

Ultimately the UK/NIF was not just about providing objective information about Y2K progress across the infrastructure. As time progressed, a public relations and political dimension evolved. First, the UK government had too much of a stake in the UK/NIF for it to seem like a failure. Second, government would have potentially instigated a form of public panic if, for instance, it had declared that the aviation sector was not 100% Y2K

compliant. Ultimately, each sector was *going* to be awarded a ‘blue light’ and declared Y2K compliant. This in itself undermined the effectiveness of the forum.

Conclusion

Preparations for Y2K were different from preparations required of a post 9/11 CIP environment. From a technological standpoint, Y2K was a more clearly defined problem *and* it had a more clearly defined solution; Y2K had a fixed and immovable deadline; and there was a clearer incentive for organisations to participate in pre-emptive economy-wide initiatives²¹. The UK/NIF and the US/WG, despite their weaknesses and blind spots, were practical responses in a specific context that brought some awareness, transparency and readiness across the infrastructure. That said, we leave its file in the 1999 file folder and ignore its lessons for 2006 at great risk to the infrastructure. Y2K offers a concrete example of a massive CIP initiative. Such enterprises are rare; it bears examining it more closely.

The US and UK Governments’ CIP plans must incorporate two facts into the centre of their approaches. First, most of the critical infrastructure is owned and operated by private industry. This means that any role the government wants to play in helping to ensure stability across the infrastructure relies significantly on its regulatory relationship

²¹ One might argue, for instance, that if one’s organisation depended on technology then one had an incentive to learn of best practices, etc., through Y2K fora. Just as important, however, one might argue that if one defected from Y2K initiatives, then others might also defect, which would increase the likelihood of a failure in one’s organisation caused by a failure somewhere along the supply chain (i.e., a ripple effect). If all organisations participated, however, such a failure was less likely, and therefore there was an incentive for every organisation to participate. With acts of terror, however, the same incentives do

with the private sector. Second, CIP has achieved a degree of complexity that challenges any template-driven cause-effect regulatory relationship. Sectors vary in cross-sector and international interdependence and potentially have significant and complex supply chains that are critical to service provision. Therefore, central control over the infrastructure is heavily constrained if not elusive.

The Marsh and Rhodes (1992) framework for Issue Networks helps to bring this second point into focus, in particular. The UK and US governments modelled their interactions with industry on corporatist and pluralist approaches, respectively. But these approaches not only embed normative assumptions about government/industry intermediation, they also have practical implications about how governments prepare the infrastructure for a crisis. The four lenses of the Marsh and Rhodes framework help us to consider not only who was involved but also how and when they were involved.

There are four observations with which to conclude. First, despite claims of complexity, fragmentation, privatisation and globalisation—common in the governance literature today—both governments straddled organisations from across the critical infrastructure and got them to work towards a common end, and achieved that end with a considerable degree of success. One important lesson that Y2K provides is that such an exercise is *possible* during peacetime.

not exist. The likelihood of attack is extremely remote yet planning for one could go on forever and absorb endless resources over time.

Second, despite both governments essentially aiming to achieve the same end, both had to rely on different policy tools and interventions to achieve that end. (See Table 3 for a summary of government interventions.) The UK government had more flexibility in its options; the US government and US owners of the critical infrastructure in general were significantly constrained by the legal context.

		Cross-Sector Co-ordination Pre-Government Intervention	Government Intervention	Cross-Sector Co-ordination Post-Government Intervention
Membership	US	Large	<i>Partner with industry associations</i>	Large, Indiscriminate
	UK	Large	<i>Select top service providers in each sector</i>	Small, Selective
Integration	US	Low	<i>Information-sharing between departments/ industry associations</i>	Fragmented and Indirect
	UK	Low	<i>Group pressure at UK/NIF</i>	Cohesive and Direct
Resource Dependency	US	Unreliable	<i>Roll-back legal constraints to encourage information-sharing</i>	Limited cross-sector disclosure
	UK	Unreliable	<i>Regulator enforces common process across UK/NIF</i>	Moderate cross-sector disclosure
Power	US	Diffuse	<i>Legislation</i>	Moderately concentrated at sector level among industry leaders
	UK	Diffuse	<i>Executive intervention</i>	Negotiated between regulators and NIF participants (industry leaders)

Table 3: Government Interventions in the Critical Infrastructure

Third, there are a number of tensions that have to be managed during initiatives that require cross-sector co-operation. There are at least two significant ones that will be noted here. First, *inter-* and *intra-*sector demands pull in opposite directions. In such an interdependent economy there was considerable interest in the Y2K status of other organisations and other sectors generally. Inter-sectoral pressures, therefore, included pressure for maximum disclosure between sectors. Within each sector, however, there was pressure to keep Y2K status un-disclosed or at least highly controlled. Organisations were trying to protect their sector's reputation collectively. In this environment, organisations wanted to keep as much information of Y2K-related disclosure as possible at the sector level only (at most).

The inter-sectoral need for transparency was only moderately successful. Intra-sector interests and institutional arrangements reinforced a strong sense of territoriality: each sector influenced strongly rule-setting and policing standards for their own sectors. The UK government was only partly able to overcome these sector-level barriers; the US government was even less able to do so. The reluctance to disclose information beyond the sector suggests that in the absence of clear incentives or *strong* and *permanent* inter-sectoral institutions, cross-sectoral co-operation seems more likely in the UK than in the US, and in fact, difficult in both.

Second, standards and markets were also held in tension although each side had its preference. Clearly the UK tipped the balance towards standards with its numerous interventions and the US tipped the balance the other way, not only by limiting its interventions, but also by rolling back the role of the state. While the US approach with its dependence on markets effectively pressured thousands of organisations towards compliance, the approach suggests two concerns for future US CIP initiatives. First, the initiatives will work much more effectively if there are clear market incentives in place for the participants. If there are not, then there is likely to be a lack of co-operation, shared focus and trust. Second and relatedly, the participants are not equally powerful, and therefore, when the government deregulates, it empowers the already powerful: smaller service providers in a highly interdependent context are likely to be bullied into adhering to the (at times) expensive sector-level standards, without recourse. One of the

challenges for the US is to create shared purpose in a market-driven environment but sufficient protections.

One role the US government played quite effectively in the run-up to Y2K was bringing attention to the issue. Becoming 'Y2K compliant' ultimately became a desirable attribute for most organisations; some banks, for instance, competed to become the first to declare themselves as compliant. Congressional hearings and the public relations strategies by the Administration helped to get Y2K in the public eye and therefore helped to create demand in the market for compliance. That noted, there are two problems the government faces when it puts so much emphasis on communications. First, the government can bring too much attention to an issue, and in so doing cause hysteria. Research suggests that the media has tended to exaggerate the likelihood of this occurring (Quigley, 2005; Clarke, 2006). The opposite reaction gets less attention but is potentially a greater threat: that the government too often brings attention to an issue and in so doing dulls the senses to the warning. How many times can the US government declare that the threat of a terrorist attack is 'code red,' for instance, before such warnings lose meaning, if they have not already done so?

In the UK, in contrast, the response was not altogether transparent. What seemed like full Y2K compliance was in fact a negotiated settlement between the regulators and a relatively small group of the regulated. For the UK, future CIP challenges will include how to bring more transparency to the work of leaders in industry, for instance, by creating fora with real authority to enforce the standards to which they claim to adhere.

Similarly, in an environment that is becoming more decentralised and fragmented, the UK government will have to develop strategies to incorporate SMEs in a meaningful and effective way into the compliance frameworks, rather than treating them in the margins and hoping for the best.

Finally, juxtaposing the two approaches underscores that, at a minimum, there are differences in approaches to CIP. In fact, the reactions by the US and UK governments', respectively, suggest a form of path dependency. Despite the increasingly populated supply chains, the UK still gravitated towards a Corporatist approach, which emphasised a relatively small number of players. And despite the US's considerable dependency on technology, in the face of a potential crisis it could not deviate from a pluralist approach, which included so many participants that it left a question mark over the economy's state of compliance right up until January 1, 2000.

The variation also suggests that any effort to standardise CIP across countries—initiatives that are gathering steam²² given the international interdependence of these key sectors—will face numerous challenges and are unlikely to be operationalised in the same manner, even if ostensibly the standards are the same.

²² GAO lists eight international CIP/Cyber-security fora of which the US government is a part. Of these eight, the UK government is a member of four (GAO, 2005, 54-55).

Bibliography

Action 2000 (1999), Final Report. Action 2000 Compact Disk. Obtained at the National Audit Office April 2004.

Adams, C. (1997), "Insurers act to stop claims over millennium bomb." Financial Times. August 20.

British House of Common Library (1998), The Millennium Bug, Research Paper: 98/72. London.

Central Computer and Telecommunications Agency (1997), Tackling the Year 2000: The Legal Implications. Cambridge: Cambridge Publishers.

Cm 4703 (2000), Modernising Government in Action: Realising the Benefits of Y2K. London: HMSO.

Committee on Public Accounts (1999), The Millennium Threat. 36th Report. London: HMSO.

Ernst and Young (1998), Millennium Infrastructure Project. Ernst and Young for Cabinet Office and obtained at the House of Commons Library.

General Accountability Office (2005A), Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. GAO-05-434. Washington DC. May.

General Accountability Office (2005B), Homeland Security: Overview of Department of Homeland Security Management Challenges. GAO-05-573T. Washington, DC. April.

General Accountability Office (2005C), Department of Homeland Security: A Comprehensive and Sustained Approach Needed to Achieve Management Integration. GAO-05-139. Washington, DC. March.

General Accountability Office (2005D), Homeland Security: Agency Plans, Implementation, and Challenges Regarding the National Strategy for Homeland Security. GAO-05-33. Washington DC. January.

General Accountability Office (2002), Homeland Security: Responsibility and Accountability for Achieving National Goals. GAO-02-627T. Washington, DC.

General Accountability Office (2001), Information-Sharing: Practices that Can Benefit Critical Infrastructure Protection. GAO-02-24. Washington, DC.

General Accounting Office (1999), Year 2000 Computing Challenge: Readiness

- Improving, But Critical Risks Remain. GAO/T-AIMD-99-49. Washington, DC.
- Marsh, D. and Rhodes, RAW (1992), "New Directions in the Study of Policy Networks." European Journal of Political Research, 21: 181-205.
- Nairn, G. (1998), "Special help for those with Y2K computer fears." Financial Times. December 2.
- National Audit Office (1999A), The Millennium Threat: 221 Days and Counting. London: HMSO.
- National Audit Office (1999B), The Millennium Threat: Are We Ready? London: HMSO.
- National Audit Office (1999C), The Millennium Threat: Is Scotland Ready? London: HMSO.
- National Audit Office (1999D), The Millennium Threat: Is Wales Ready? London: HMSO.
- New York Times Editorial Desk, (1999A), "Liability for the Millennium Bug." New York Times. April 26.
- New York Times Editorial Desk (1999B), "Liability Limits." New York Times. July 3.
- President's Council on Year 2000 Conversion (2000), The Journey to Y2K: Final Report. Downloaded from www.y2k.gov/docs/lastrep3.htm.
- Quigley, K. (2005A), "Bug Reactions: Considering US Government and UK Government Operations in Light of Media Coverage and Public Opinion Polls." Health, Risk & Society. 7:3, 267-291.
- Quigley, K. (2005B), "Risk Regulation Regimes in Aviation: Were the Chips Ever Really Down in the UK's Management of Y2K?" in I. Demirag (ed.) Corporate Social Responsibility, Accountability and Governance: Global Perspectives. Sheffield: Greenleaf.
- Rhodes, R.A.W. (1997), Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability. Buckingham: Open University Press.
- Schmitter, P. (1979), "Still the Century of Corporatism?" Trends Towards Corporatist Intermediation. 7-52. London: Sage.
- Simons, J. (1999), "Trade Groups and Companies Join Forces to Push Limited Y2K Liability." Wall Street Journal, Feb 3.
- Standing Committee on Science and Technology (SCST) (1997/98), The Year 2000

Computer Compliance, Second Report to the House of Commons. London: HMSO.

Taylor, P. (1998), “Standards and SEC.” Financial Times. September 1.

Taylor, P. (1999), “Millennium bug fails to materialise.” Financial Times. October 9.

United States Senate Special Committee on the Year 2000 Technology Problem (1999), Investigating the Impact of the Year 2000 Problem (February Committee Report). Washington DC. Obtained at: www.senate.gov.

Vogel, D. (1986), National Styles of Regulation. New York: Cornell University Press.