Routledge
Taylor & Francis Group

The International Spectator
Italian Journal of International Affairs

ISSN: 0393-2729 (Print) 1751-9721 (Online) Journal homepage: https://www.tandfonline.com/loi/rspe20

The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security

Lindy Newlove-Eriksson, Giampiero Giacomello & Johan Eriksson

To cite this article: Lindy Newlove-Eriksson, Giampiero Giacomello & Johan Eriksson (2018) The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security, The International Spectator, 53:2, 124-140, DOI: 10.1080/03932729.2018.1458445

To link to this article: https://doi.org/10.1080/03932729.2018.1458445

Published online: 29 May 2018.

THE INTERNATIONAL SPECTATOR, 2018
VOL. 53, NO. 2, 124–140
https://doi.org/10.1080/03932729.2018.1458445

The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security

Lindy Newlove-Eriksson[a], Giampiero Giacomello[b] and Johan Eriksson[c]

[a]Royal Institute of Technology (KTH) and Swedish Defence University (SEDU), Stockholm; [b]University of Bologna; [c]Södertörn University, Stockholm

ABSTRACT

Corporatisation of critical information infrastructure (CII) is rooted in the 'privatisation wave' of the 1980s-90s, when the ground was laid for outsourcing public utilities. Despite well-known risks relating to reliability, resilience, and accountability, commitment to efficiency imperatives have driven governments to outsource key public services and infrastructures. A recent illustrative case with enormous implications is the 2017 Swedish ICT scandal, where outsourcing of CII caused major security breaches. With the transfer of the Swedish Transport Agency's ICT system to IBM and subcontractors, classified data and protected identities were made accessible to non-vetted foreign private employees – sensitive data could thus now be in anyone's hands. This case clearly demonstrates accountability gaps that can arise in public-private governance of CII.

KEYWORDS

Critical infrastructures; public-private partnership; privatisation; computer networks; outsourcing; remote management; Swedish ICT scandal

In order to produce, operate and distribute public services and goods to citizens, modern, post-industrial societies rely on complicated logistics systems and intricate asset network architectures. Critical infrastructures can be likened to the arteries and veins of human beings, without which it would be quite impossible for them to function. Essentially, this is why infrastructures such as those for energy, transport, communications and financial services are defined as *critical*.[1] As large and complex systems, catastrophic effects could follow if they were to break down.[2]

Due to rapid technological development and increasing dependence on information and communications technology (ICT), most of these infrastructures are now operated, managed and/or controlled via interconnected computer networks and information flows, so that they have essentially become critical *information* infrastructures (CII).[3] Elaborating on the body metaphor, this can be seen as the equivalent of adding nerves to the arteries and veins. In the past, destroying or even disrupting physical infrastructures required

CONTACT Lindy Newlove-Eriksson lindy.newlove-eriksson@fhs.se

[1]Cohen,"What makes critical infrastructures *critical*", 53-4.
[2]Perrow, *Normal Accidents*; de Brujine and van Eeten, "Systems that should have failed"; Metzger, "Concept of critical infrastructure protection".
[3]Dunn-Cavelty and Suter, "The Art of CIIP Strategy".

substantial resources and energy, as demonstrated, for example, by the Allies' bombing campaign against Germany in World War Two.[4] Currently, essentially all infrastructures are 'cyber-physical', that is, ICT-controlled: if some computer nodes were put out of service via cyber attacks or other causes, cascading effects could negatively impact various integral areas of contemporary societies, from healthcare to power and transport. It is therefore hardly surprising that the protection of CII is a paramount element of cyber security.

Governments were formerly the sole or principal owners and operators of such critical infrastructures. This organisational praxis went chiefly unchallenged, until economists, policymakers, entrepreneurs and the public – inspired by the neoliberal turn – began to contemplate and address 'how much' governments should 'own' of the economy. Thus other stakeholders entered and progressively came to dominate infrastructural property and operation. The 'go-private' option has prevailed in recent decades and corporate practices have increasingly been applied to CII management. At the same time, however, the private sector has proven to be rather reluctant to tackle the 'security' dimension and vulnerabilities of CII,[5] with at times dire consequences, as demonstrated by the topical Swedish case study presented here.

Against this background, the article addresses how the commercialisation of CII, that is, the business practices including commodification and outsourcing of public services and the implementation of market principles within public administrations can impact on politics and national security. Following this introduction, we discuss the general development of CII and the global 'privatisation wave' that began in the late 1970s in post-industrial economies. Subsequently, we conduct a case study of the 2017 Swedish ICT scandal as a key empirical illustration of the more general trends and problems of public-private partnership in CII.[6] In this case, it was revealed that the Swedish Transport Agency had outsourced its entire ICT system to IBM and subcontractors of the computer conglomerate in Eastern Europe, giving unvetted foreign and private employees full access to massive amounts of secret and highly sensitive data on, among other things, core Swedish CIIs. The result was one of the worst political crises this Scandinavian country has ever experienced.

While there is still much discussion about how vulnerable CIIs actually are,[7] there is consensus that major disruption of CII would generally have numerous grim consequences for society and government. In addition, given cross-sectoral interconnectedness through joint ICT systems, breakdown of safety and security of one or more CIIs would likely have 'ripple effects' on other critical national infrastructures, thus creating the possibility of cascading disasters.[8] Furthermore, although CIIs are mostly developed and built at the national level, they are interconnected with other countries' infrastructures and thus a breakdown in one place is likely to impact negatively on neighbouring countries and regions as well.[9] A major European example, elicited by linked socio-technical and economic

[4]Newland and Chun, *The European Campaign*, 112-30.
[5]Kaplan, *Dark territory*, 102-5; van Eeten and Bauer, "Emerging threats to internet security".
[6]Andersson and Malm, "Public–private partnerships and challenge".
[7]Dunn Cavelty and Suter, "Public–private partnerships"; Metzger, "Concept of critical infrastructure protection"; Lukasik *et al*., *Protecting Critical Infrastructures Against Cyber-Attack*.
[8]Pescaroli and Alexander, "Critical infrastructures, panarchies".
[9]Note that the distinction between 'critical infrastructures' and 'critical information infrastructures' is that in the latter the emphasis is on computers and networks that permit remote control and management of physical infrastructures (cf. Dunn Cavelty and Suter, "The Art of CIIP Strategy").

factors was the 2006 blackout which caused electricity outages for approximately 15 million households as well as trains and other critical infrastructures in northern Germany, Belgium, France, Spain and Italy.[10]

Moreover, the vulnerability and security implications of interconnected CII are further aggravated by fragmentation of governance through commercialisation. Privatisation and outsourcing are highly influential in contemporary CII governance in many countries. However, while the intention is ostensibly to increase efficiency and keep public expenditures down, the effects of these forms of fragmented governance can be devastating in terms of security and public accountability.[11] These effects are clearly illustrated by the Swedish case study examined herein.

Interconnected critical information infrastructures

What is considered CII is fairly similar across the world, despite some terminological differences between, for example, the US, the EU, and other economically advanced countries such as Japan, Australia, Canada and South Korea.[12] The US National Institute of Standards and Technology (NIST) defines critical infrastructures as those

> systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[13]

Likewise, the European Commission (EC) describes critical infrastructures as

> physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU States.[14]

Control mechanisms of various types connect infrastructures at multiple points, particularly through joint ICT systems for information-sharing and communication. Moreover, because of the transnational integration of critical infrastructure within the EU, each government must also consider how their national systems are affected by cross-border incidents, and how their own systems impact on that of other member states.

Any government would likely acknowledge that critical infrastructures crisscross many sectors, including banking and finance, transport and distribution, energy, utilities, health, water, food supply and communications, as well as key government services. But there is clearly a 'hierarchy' of infrastructures, in the sense that the malfunctioning of integral 'key' services tends to 'cascade' down on other CIIs. Unsurprisingly, electric power and telecom are "the most critical infrastructures, on which virtually all the others depend".[15] In particular, power generation and distribution is effectively one of the most essential infrastructures, the failure of which impacts on all other CII, as amply demonstrated.[16]

[10]Plietzch *et al*., "Local vs global redundancy".
[11]Grimsey and Lewis, "Evaluating risks of public private partnership".
[12]Abele-Wigert and Dunn, *International CIIP Handbook 2006*.
[13]Kissel, *Glossary of Key Information Security Terms*.
[14]Fritzon *et al*. "Protecting Europe's critical infrastructures".
[15]Lukasik *et al*., *Protecting Critical Infrastructures Against Cyber-attack*, 7; cf. Hellström, "Critical infrastructure and systemic vulnerability".
[16]See Antonsen *et al*., "Reliability consequences of liberalization", as well as empirical research: Plietzch *et al*., "Local vs global redundancy"; Miller *et al*., "Hazards of neoliberalism"; Almklov and Antonsen, "The commoditization of societal safety"; Palm, "Emergency management".

The security of CII is typically framed in terms of reliability and resilience (e.g. via redundancy/duplication). Security of infrastructure however, is often considered in terms of an archetypical economic externality. As with pollution, externalities produce collective/societal problems without motivating sufficient private action, and it is unclear who should bear their costs. If the cost of failure is not borne directly by the owners/operators of infrastructure, incentives to improve conditions are few.[17] Presently, if a utility operating in conjunction with CII were to suffer failure, its management could argue exceptionality, i.e. their expected obligations of service were exceeded.[18] It could even be contended that the fault was the result of a hostile act by a foreign power, thus the immediate default responsibility would be shifted to the government, which has the responsibility to defend against foreign nationals, not the private sector. Similarly, cybercrime – that is, when a computer is the object of the crime or is used as a tool to commit an offence – typically falls under the domain of law enforcement and is the responsibility of state actors.

The invisible hand?

Since the 1970s, privatisation has been recognised as one of the most influential economic policy reforms.[19] Continuing in the 1980s and early 1990s, proponents regarded cutting costs of formerly public assets as imperative and cultivated an organisational culture that often viewed replication as wasteful. Hence, private companies providing (formerly public) utility services might consider redundancy/replication of control systems as uneconomical, and not divert revenues from stakeholders to increasing infrastructure resilience, especially to counter remote or unlikely events.

Critiques of state-led development strategies from the mid-1970s onwards began to question national economic control and seek heightened efficiency. Scholars, economists, entrepreneurs and policymakers were keen on finding alternatives that might solve the problems of the perceived failure of state ownership strategies.[20] Answers were often found in 'privatisation', the ceding of state functions and/or assets, in full or in part, to private actors.[21] There have been many organisational variants of privatisation, but management through market mechanisms and commoditisation of services is a common denominator.[22] It entails, as put by Christopher Sheil,[23] the ultimate 'corporatisation' of the public sector.

Until Margaret Thatcher's conservative government came to power in Great Britain in 1979 and Ronald Reagan became US President in 1981, the conventional wisdom was that "the government should at least own the telecommunications and postal services, electric and gas utilities, and most forms of non-road transportation (especially airlines and

[17]Kaplan, *Dark territory*, 102; Almklov and Antonsen, *Ibid*.; Abele-Wigert, "Challenges governments face"; Ryu *et al*., "Reducing security vulnerabilities".
[18]An interesting document comparing how some US/Canadian companies can avoid/be exempt of liability for failures of their utility services is provided by a document of BC Hydro (a Crown corporation, owned by the government and people of British Columbia) "Various Utilities' Liability/Exemption Clauses", www.bchydro.com/content/dam/hydro/medialib/internet/documents/news/press_releases/appendix3_vanoutageotherliability2008.pdf.
[19]Clifton *et al*., "Privatizing public enterprises"; Block and Somers, *The Power of Market Fundamentalism*.
[20]Henry, "The wave of privatization".
[21]Donahue, *The privatization decision*; Fitzgerald, *When government goes private*; Vickers and Wright, "The politics of industrial privatization".
[22]Antonsen *et al*., "Reliability consequences of liberalization"; Almklov and Antonsen, "The commoditization of societal safety"; Brendan, *In the Public Interest*.
[23]Sheil, *Water's fall*.

railroads)".[24] In the mid-1980s and early 1990s, however, the path to better – that is more efficient – industry governance was thought to be a one-way street via commercialisation, particularly privatisation.[25]

Despite widespread criticism,[26] many governments continue to endorse neoliberal economic policies in this field.[27] Indeed, each country has moulded its privatisation process on its own entrepreneurial and business culture.[28] In post-communist countries previously dominated by rentier economies, for example, privatisation was presented to governments as a *tool* for improving efficiency and the quality of public administration.[29]

The strong belief in the 'invisible hand' of the market and its efficiency with respect to lowering costs and allocating resources gave birth to 'supply-side economics' which stress that the most significant and efficient way of allocating resources is via decentralised, individual, competitive private decision-making, and not via centralised, collective public sector decision-making.[30] The Thatcher and Reagan governments, both strong supporters of the neoliberal ideology, contributed to exporting it to developing countries, Eastern Europe, the Soviet Union, the OECD and other communities.

It has been shown that cost-effectiveness may improve when competitition is real, requiring market shares to be split among many different actors; however, where monopolies or oligopolising tendencies predominate, cost-effectivness tends to be stifled and the positive effects of markets and competition lost.[31] Furthermore, the logic of cutting costs to increase profit in newly privatised infrastructures poses problems with respect to CII, as resilience of network utilities is often achieved by duplicating (or ideally triplicating) controls, monitoring and safety mechanisms. Redundancy is acknowledged as being critical to safety in complex systems; when initial control devices fail, there ought be a second and perhaps even third system in place. For example in the aviation industry, where aircraft typically have two backup control systems (in addition to the main one), redundacy is recognised as vital for safety and security. The private sector however, often lacks the intention – and incentives – to invest in redundancy.

In an age of mounting risk and re-insurance, governments that may even have benefited from the privatisation of public utilities – at least in the short term – are reluctant to shoulder costs singlehandedly. In any case, in the event of CII failure and cascading disasters, it will chiefly be governments that will have to 'foot the bill' after their citizens suffer the consequences of poor preparedness and mitigation. This is an example of what Jenny Palm calls "responsibility gaps", which arise between public and private actors when responsibility for long-term planning and emergency management is shirked.[32]

[24]Megginson and Netter, "From state to market", 323.
[25]Savas, *Privatization: Key to better government*; Brendan, *In the Public Interest*.
[26]Dixon and Kouzmin, "Public domains, organizations"; Vickers and Wright, "The politics of industrial privatization".
[27]Pirie, *Privatization: Theory, practice and choice*; Savas, *Privatization: Key to better government*.
[28]Linder, "Coming to terms with"; Feigenbaum and Henig, "Political underpinnings of privatization".
[29]Pirie, *Privatization: Theory, practice and choice*; Savas, *Privatization: Key to better government*.
[30]E.g. Donahue, *The privatization decision*; Fitzgerald, *When government goes private*; Redenius, "The supply-side alternative"; Block and Somers, *The Power of Market Fundamentalism*.
[31]See for example Hodge and Greve, "Public–private partnerships"; Megginson and Netter, "From state to market"; Porter, "When Public Outperforms Private"; Jones, "Why Britain's Trains Don't Run"; "Public Works, Private Benefit", *The New York Times*, 9 June 2017, A26; Goodman, "Infrastructure Goes Private", B1; Goodman and Lovemen, "Does privatization serve the public interest?"; Dixon *et al*., "The dilemma of privatized public services."
[32]Palm, "Emergency management".

Outsourcing CI as a violation of national security: the 2017 Swedish ICT scandal

Having identified the general features of interconnected and increasingly commercialised CIs, it remains to be seen how they play out in practice. To illustrate this, we examine the recent Swedish national ICT scandal. On 7 July 2017, the lull of the Swedish summer holiday season turned into a political hurricane as the Swedish newspaper *Dagens Nyheter* revealed major violations of laws and security protocols at the Swedish Transport Agency (*Transportstyrelsen*). This case is particularly interesting for two reasons. First, it shows how outsourcing for the purpose of cost-effectiveness was explicitly prioritised over national security, which in this case had major legal, political and security implications. Second, this case is precisely about cross-sectoral interconnectedness of CI, in technology and in public-private governance. The Swedish Transport Agency has a core function in managing and coordinating highly classified information regarding several CIs, including transportation systems, roads, railroads, airports and harbours. Moreover, the agency is also responsible for the national registry of drivers licenses and the national vehicle registry, as well as the identities of secret agents within the military and the police, and some police investigative databases.[33]

The national scandal exploded when it was revealed that, since 2015, the agency – breaking several laws as well as the agency's own rules – had outsourced the management of its top-secret databases and entire ICT system to subcontractors of IBM. This violation allowed non-vetted private employees in Serbia, Romania, Hungary and the Czech Republic, none of whom had security clearance, to access highly sensitive Swedish information.[34] Later, it was revealed that Swedish authorities had outsourced the ICT systems not only of the transport sector, but also of large parts of the Swedish medical system, which meant that private sector employees based in Eastern Europe were given access to private and confidential information on the medical status of Swedish citizens.[35] While it was initially stated that around 20 foreign individuals had received access to the sensitive data, it turned out later that around 80 non-vetted people in several Eastern European countries had full access to all systems. Moreover and remarkably, these non-vetted foreign private sector employees retained their illegitimate access for several months after the scandal broke. The governmental and legal investigation that followed confirmed that massive amounts of top secret information had been leaked without any knowledge of where or to whom it had been dispersed.[36] When the scandal was exposed by Swedish media, the government quickly said it wanted to "insource" rather than "outsource" the management of ICT-connected CIs. But by then the damage had been done.

[33]Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [*Mapping the handling of certain information*].
[34]Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017]; Örstadius, "Maria Ågren nekar till brott" [Maria Ågren claims not guilty]; Delin, "IBM vägrar att svara" [IBM refuses to respond]; Milne, "Sweden grapples with huge leak"; Griffin, "Sweden leaks details".
[35]Holmberg "Läkarförbundet" [Swedish Medical Doctors Association].
[36]"Obehöriga hade tillgång till hemliga uppgifter så sent som i höstas" [Unauthorized people had access to secret information], *Dagens Nyheter*, 23 January 2018; Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [Mapping the handling of certain information], 11.

What happened?

In 2014, the Swedish Transport Agency was looking to replace its ICT system, which included storage and management of sensitive and highly classified information on core Swedish CIs. Until then, the Swedish Transport Agency's ICT system and databases had been under the jurisdiction of the Swedish Transport Administration (*Trafikverket*), a related agency with responsibility for long-term planning of the transport system for all types of traffic, as well as the building, operation and maintenence of public roads and railways, and for the administration of drivers licenses. In seeking a new ICT system, the Transport Agency decided on a competitive bid on the private market[37] – an approach wholly in line with the New Public Management philosophy that had influenced public administrations in the West for years, not least in Sweden.[38] Indeed, over the last two decades, Swedish governments have outsourced the provision of many public services, motivated by the belief that this is a way to increase effiency and cost-effectiveness.[39]

In March 2015, the Director General of the Transport Agency retired. The newly-elected Swedish government, led by Social Democratic Prime Minister Stefan Löfven, appointed Maria Ågren as the new Director General of the Transport Agency. Notably, she was appointed with the explicit task of increasing efficiency and accelerating the outsourcing of the agency's services to private companies.[40] Two months after Ågren became Director General, a global leader in ICT – IBM – won the bid for creating *and managing* the agency's new ICT system, including all the sensitive databases and control systems for core Swedish CIs. A contract worth approximately USD 94 million was quickly signed and implementation immediately undertaken.[41]

In the summer of 2015, security staff at the Transport Agency repeatedly expressed their concerns about how the new management was sidestepping security routines and directives – worries that were eventually communicated to the National Security Police (*Säpo*).[42] In early 2016, the National Security Police initiated an investigation on how the Transport Agency was handling sensitive information, but this investigation was kept secret from the media and the public. The Transport Agency ignored the warnings, the handover to IBM continued as planned, and less than a month later the transfer of data and the outsourced systems were in place.

In January 2017, the government fired Ågren, only stating at that time that the Minister of Infrastructure Anna Johansson and Ågren had "different views on how to conduct the work".[43] This allegedly came as a complete surprise to board members of the agency, and the

[37]Örstadius, "Maria Ågren röjde sekretessbelagda uppgifter" [Maria Ågren revealed top secret information] and "Nya dokument från Maria Ågren" [New documents from Maria Ågren].

[38]New Public Management (NPM) draws on neoliberal ideology and public choice theories, implying use of markets and competition in public administration and the provision of public services. It emphasizes performance, productivity, efficiency, outputs, commodification of services, and a treatment of citizens and civil servants as 'customers' and 'clients'. Hall, "NPM in Sweden"; Eliner and Jordahl, "Political preferences and public sector outsourcing".

[39]Hall, *Ibidem*; Statskontoret [Swedish Public Administration Agency], *Att göra eller att köpa? Om o outsourcing av statlig kärnverksamhet [To do or to buy? On outsourcing of core public services]*. http://www.statskontoret.se/upload/Publikationer/2015/Om-offentlig-sektor_23_Outsourcing.pdf.

[40]Svahn, "Säpos tillsyn avslöjade brottet" [Säpo's review revealed the crime]; Örstadius, "Nya dokument från Maria Ågren" [New documents from Maria Ågren].

[41]Örstadius, "Ågren sparkades" [Ågren fired]; Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017]; Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [Mapping the handling of certain information].

[42]Svahn, "Säpos tillsyn avslöjade brottet" [Säpo's review revealed the crime]; Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017]; Örstadius, "It-skandalen på Transportstyrelsen" [IT scandal at Transport Agency].

[43]Svahn, *ibid*.; Örstadius, "Maria Ågren nekar till brott" [Maria Ågren claims not guilty]; Brevinge, *ibid*.

reason given merely pointed to general disappointment with her work, not to any specific concerns.

On Friday, 7 July 2017, the Swedish daily *Dagens Nyheter* suddenly revealed the true reason why the Director General had been fired and eventually fined. This was that she had put national security at risk by outsourcing secret and sensitive information and ICT control to private and foreign actors with no security clearance. This was confirmed by the public investigation that followed. Ågren later admittted that she had sidestepped security procedures during the outsourcing of Swedish ICT, but only "to avoid media exposure" (it remains unclear if she meant exposure for herself, for the government, or both), and that the government had been fully informed.[44] This was breaking news as it revealed not only a national security crisis but also a major cover-up by the Swedish government.[45] The whole matter quickly turned into one of the biggest political scandals the country has ever experienced, and soon caught the attention of the international media.[46]

The political opposition parties rallied and demanded that the responsible ministers resign, specifically the Minister of Infrastructure Johansson, Minister of the Interior Anders Ygeman, and Defence Minister Peter Hultqvist. Just prior to the vote of confidence for these ministers in Parliament, however, Prime Minister Löfven announced a reshuffling of his cabinet, excluding Johansson and Ygeman.[47] The Defence Minister stayed on as he is popular among members of the political opposition, and he subsequently survived the vote of confidence.[48] It was also decided that the Constitutional Committee of the Parliament would conduct a thorough enquiry into the entire affair.

Efficiency prioritised over national security

In this case, there is not merely a suspicion that efficiency and cost-effectiveness were prioritised over national security, it is a verified fact. Indeed, the Director General of the Swedish Transport Agency herself admitted that she had commanded the agency to speed up the outsourcing and skip the standard and time-consuming security clearance procedures. She did so by signing a document entitled "Exception from active legislation", in which she clearly spelled out that security clearance was not needed, despite critique from her own staff as well as from the National Security Police. Reportedly, a member of the ICT security staff at the Transport Agency said during the subsequent legal investigation that "it felt pretty hopeless", it was obvious that the agency was "doing the wrong thing", but that "nobody seemed to care".[49]

Moreover, the Swedish State Service Center (SSC), a government agency with the task of assisting other agencies in improving cost-effectiveness, and Swedish news media revealed

[44]Örstadius, "Nya dokument från Maria Ågren" [New documents from Maria Ågren], "It-skandalen på Transportstyrelsen" [IT scandal at Transport Agency], and *ibid*.
[45]Örstadius, "Regeringskansliet lägger locket" [The government cover things up]; Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017].
[46]Griffin, "Sweden leaks details"; Milne, "Sweden grapples with huge leak"; Anderson, "Swedish Government Scrambles.
[47]"Statsminister Stefan Löfven ombildar regeringen efter misstroendeförklaringen" [Prime Minister Stefan Löfven rebuilds cabinet after the vote of confidence], *Dagens Nyheter*, 29 July 2017.
[48]Larsson, "Peter Hultqvists försvar" [Peter Hultqvist's defence].
[49]Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017]; Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [Mapping the handling of certain information].

that around 40 national public agencies had outsourced their ICT systems and services.[50] In the wake of the ICT scandal, a series of critical commentaries emerged, all of them essentially condemning the lack of security culture, and general ICT incompetence in the Swedish public administration as well as in Parliament and among the political parties represented there.[51]

Ågren claimed that if all rules and security routines had been followed, the transition to a new ICT system (to be run externally by IBM) would have been delayed for so long that the old system would have been obsolete before the new one was in place.[52] She put the blame on the government which, she claims, pressured her not to slow down the outsourcing process. In fact, as soon as Ågren got the job, she was called to a meeting with Erik Bromander, Undersecretary of Infrastructure, who allegedly emphasized that it was "necessary" that "the projects [be] fulfilled according to plan", i.e. the rapid outsourcing of Swedish ICT.[53] Interestingly, IBM remained mute throughout the entire scandal. They forwarded all questions to the Swedish Transport Agency, and simply stated that they had fulfilled their obligations according to their contract.[54]

The legal investigation revealed that in addition to violation of the Transport Agency's own rules and routines, no less than three Swedish laws were violated: the Security Protection Law (*Säkerhetsskyddslagen*), the Personal Information Law (*Personuppgiftslagen*), and the Law on Publicity and Secrecy (*Offentlighets- och sekretesslagen*). Accordingly, Ågren was prosecuted and found guilty of violating national security, resulting in a hefty fine but no further legal action.[55]

Not only the opposition, but also the Prime Minister and other members of the Swedish cabinet reacted by strongly condemning how efficiency had been prioritised over national security. When the news broke, Prime Minister Löfven was initially silent, forwarding all questions to the Minister of Infrastructure Johansson. When Löfven finally went public, he stated that what had happened at the Transport Agency was a "disaster". He also claimed that he had not been informed about it until January 2017, when he then took the decision to fire the Director of the Transport Agency.[56] The news media revealed that both the Defence Minister and the Minister of Internal Affairs had known about the violation of security as early as 2016, but that neither of them had forwarded this information to the Prime Minister or the Minister of Infrastructure.[57] In July 2017, it was also revealed that the Ministry of Justice had been informed as early as September 2015, which was just before the IBM subcontractors took over ICT management. Prime Minister Löfven replied that the Ministry of Justice is responsible for how they received and communicated information. Thus, the Prime Minister tried to allocate accountability to the Ministry of Justice. From a critical point of view, the Prime Minister cannot avoid overall accountability, both given his

[50]"40-tal myndigheter har outsourcat it-drift" [Some 40 public agencies have outsourced IT services], *Dagens Nyheter*, 31 July 2017; Darab, "Statens Servicecenter varnade regeringen" [National Service Center warned government].
[51]E.g. Qviberg, "It-kompetensen är obefintlig" [IT competence is nonexistent]; Larsson and Qvist, "Säkerhetsexperterna Dan Larsson och Peder Qvist" [Security experts Dan Larsson and Peder Qvist]; Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [Mapping the handling of certain information: report], 15.
[52]Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017].
[53]Örstadius, "Nya dokument från Maria Ågren" [New documents from Maria Ågren].
[54]Delin, "IBM vägrar att svara" [IBM refuses to respond].
[55]Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [Mapping the handling of certain information]; Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017].
[56]De la Reguera, "Stefan Löfven om Transportstyrelsens it-skandal" [Stefan Löfven on Transport Agency's scandal].
[57]Brevinge, "Regeringskrisen i juli 2017" [The government crisis in July 2017].

power over all of his ministries and the fact that the ICT scandal involved several ministries. As noted, this clearly illustrates CII as a cross-sectoral problem.[58]

Blame games might be unavoidable when a scandal of such proportions is revealed.[59] Yet, they shift attention from underlying structural problems to actors. Indeed, as much as specific individuals were found to be guilty of violating laws and directives, the fragmentation of control and accountability, and the larger culture and praxis of outsourcing can arguably be implicated in this case. A look at these factors is therefore essential for understanding both this case and the security implications of contemporary CI governance more generally. As put in a critical piece, journalist Niklas Ekdal claimed that this was not a conspiracy but rather an expression of naiveté:

> In the dog days of 2017 […] an intelligent octopus has been replaced by a mindless jellyfish that swims with the tide. Instead of authoritarian hush-hush in the deep state, we have a mute public administration in which no one seems to have full oversight or talk to anyone else.[60]

Indeed, Prime Minister Löfven himself suggested that "a naiveté has probably existed for far too long concerning outsourcing" – a statement explicitly referring to the Swedish public administration in general, not only the Swedish Transport Agency. Importantly, this naiveté, expressed in terms of a weak security culturre and lack of security expertise, was confirmed by the official investigation that followed.[61]

Put more provocatively, it seems that the public administration is run more by culture and praxis than by civil servants with discreation to act and think responsibly. The Swedish IT scandal can be interpreted as a consequence of a New Public Management (NPM) culture which has shaped the Swedish public administration since the 1980s, as convincingly demonstrated by past research.[62] This culture distrusts the efficiency of public administration, favouring private and commercialised solutions – including outsourcing of services, and management information.

Notably, the Swedish NPM culture has been adopted across party lines, and implemented by both centre-right and Social Democratic governments, as opposed to Denmark, for example, where Social Democrats have opposed market-type reforms.[63] In this case of the outsourcing of ICT systems and other CIs, it was the Social Democratic government in power that insisted on outsourcing the systems. Yet it had also been advocated by the preceding centre-right government, which had already stated in 2011 that "it is desirable that a major part of the ICT systems of public administrations be outsourced", and that "normally public administrations should not provide their own ICT systems", although it also noted that "information security" had to be taken into consideration.[64]

As shown very clearly by the Swedish ICT scandal, public services can be outsourced, but public accountability cannot. At the end of the day, public officials will be held accountable,

[58]De la Reguera, "Stefan Löfven om Transportstyrelsens it-skandal" [Stefan Löfven on Transport Agency's scandal]; "Säpoveto ska hindra nya it-skandaler" [Säpo veto will prevent new IT scandals], *Dagens Nyheter*, 9 September 2017.
[59]Boin *et al*., *The Politics of Crisis Management*.
[60]Ekdahl, "It-läckaget på Transportstyrelsen" [IT leak at Transport Agency].
[61]De la Reguera, "Stefan Löfven om Transportstyrelsens it-skandal" [Stefan Löfven on Transport Agency's scandal]; Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [*Mapping the handling of certain information*], 15.
[62]Cf. Hall, "NPM in Sweden"; Eliner and Jordahl, "Political preferences and public sector outsourcing".
[63]Green-Pedersen, "New Public Management reforms".
[64]Against this background, it is not surprising that not only current Social Democratic and Green Party ministers, but also members of the former centre-right cabinet have been called to hearings before the Constitutional Committee. Hoff, "KU-anmälning 2017" [Report to the Constitutional Committee 2017]; Wilhelmsson, "S-ledamoten Hans Hoff" [Social Democratic MP Hans Hoff].

even if public services have been outsourced. While outsourcing facilitates blame games among public and private actors, the Swedish ICT scandal shows that, at least in this case, accountability finally rests with public authorities and, ultimately, the democratically elected government. Interestingly, the risk of security leakages as well as accountability problems associated with outsourcing were noted in a critical public report already in 2011.[65] Apparently, this was not enough to prevent the crisis. Of course, a different Director General might have handled outsourcing differently than Maria Ågren, and made sure that private employees were vetted before getting access to secret information. Yet, without the NPM culture prioritizing marketization over national security, it is likely that neither ministers nor Director Generals would have been able to do what now was done.

From outsourcing to insourcing?

How, then, did the government deal with the situation of the outsourced ICT systems and security leakages? Early on after the scandal was revealed, several government representatives, including the Minister of Public Administration, Ardalan Shekarabi, started talking about "insourcing what had been outsourced". Shekarabi stated very clearly that for "particularly sensitive information and services, outsourcing is not appropriate".[66] It was thus declared that the outsourcing would end, and that the ICT systems and all sensitive information would be brought back to Sweden and put under state-run management.[67] It was also revealed that in practice, insourcing could not be done overnight, but would take several months.[68] Since 1 October 2017, only Swedish staff with security clearance has access to the outsourced databases and secret information.[69]

Thus, a reframing seems to have occurred, in which the long-running New Public Management discourse on commercialisation and effectiveness was at least temporarily rejected. More specifically, in July 2017, the government assigned the Swedish Post and Telecom Authority (PTS) to work on a model for secure ICT systems for public authorities. At the same time, earlier proposals came back on the agenda, such as establishing secure and *state-run* 'server halls' in Sweden in which all sensitive information would be stored, and setting up special government 'cloud' services.[70] These revamped ideas also received backing from the National Security Police, the National Authority for Signals Intelligence, and the National Defence Radio Establishment, among others. Moreover, in September 2017, the government proposed that the Security Police should have the power to veto the outsourcing of security-sensitive activities and information.[71]

Hence, at least at the rhetorical level, the Swedish government seems to have turned from outsourcing to insourcing. It remains to be seen whether this will be followed up in practice. As previously indicated, highly sensitive classified information remained in the hands of unvetted private sector non-nationals for months after the scandal broke, until late Fall 2017. Moreover, it is as yet unclear whether the insourcing response to the recent ICT scandal is

[65]Riksrevisionen [National Audit Office], "IT inom statsförvaltningen" [IT within the state administration].
[66]"Offentlig it-säkerhet ska förbättras" [Public IT Security will be improved], *Dagens Nyheter*, 27 July 2017.
[67]*Ibid*.
[68]Kallvinge, "Återföringen av it-driften" [The insourcing of IT services]; Anderson, "Swedish Government Scrambles".
[69]Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter* [*Mapping the handling of certain information*], 11.
[70]Darab, "Statens Servicecenter varnade regeringen" [National Service Center warned government]; "Offentlig it-säkerhet ska förbättras" [Public IT Security will be improved], *Dagens Nyheter*, 27 July 2017.
[71]"Säpoveto ska hindra nya it-skandaler" [Säpo veto will prevent new IT scandals], *Dagens Nyheter*, 9 September 2017.

a sign of a broader policy change or if this is the exception that proves the rule regarding the dominance of outsourcing and other features of the New Public Management culture.[72] Given the widespread use of outsourcing and public-private partnerships in Sweden (and elsewhere in the West), further security violations and political scandals cannot be ruled out. The New Public Management culture and praxis, which prioritises efficiency over national security, may not entirely have loosened its grip on Swedish society.

Conclusion

In 2017, commenting on US President Donald Trump's plan to rejuvenate infrastructures in the United States via the private sector, the *New York Times* concluded that "handing profit-making companies responsibility for public works can produce trouble".[73] Likewise, another observer noted: "privatization of the utilities and the adoption of 'Just in Time' delivery techniques for food and fuel means there is very little 'give' in the system to cater for unexpected events".[74]

Whereas many might back the claim that "[r]esearch now supports the proposition that privately owned firms are more efficient and more profitable than otherwise comparable state-owned firms",[75] this observation is squarely concerned with profits and cost-effectiveness. National security is clearly not part of that equation, as exemplified by this case study. In effect, not all sectors are the same; owning and operating a taxi or chocolate company is not the same as managing energy supply or public transport.

Further, in protecting CIIs, attention must be given to both anticipation and resilience. Effective anticipation, however, is increasingly difficult when critical infrastructures are both interconnected and less controlled by central governments. With networks, webs and grids all interconnected through joint ICT systems, cascading effects make effective anticipation almost impossible. Resilience through redundancy is also difficult to achieve as it comes with additional costs, which only pay off if and when a disaster occurs. When utilities and other critical infrastructures are solely in public hands, demands for greater investment to increase security are more easily met, although all societies must now grapple with the zero-sum game of public allocation of limited resources. With multiple stakeholders, however, all parties involved agree on cutting costs, but typically disagree on who should bear the pricetag for risk reduction in CII. Cloud computing has arguably exacerbated issues of both quantification and traceability of risk.

Moreover, when things go awry in public-private constellations, blame games will surely follow, in which most actors believe they have a chance of escaping at least some of the responsibility.[76] On the one hand, for corporate actors, utilities that are part of CIIs (e.g. water and power distribution) are public goods, and therefore it is the state that should bear the brunt of greater investment for security requirements. At the same time, however, the private sector is adamant about sharing profits (and the public funding) that may be generated by managing public utilities. On the other hand, privatising was and still is perceived as a way to save resources and increase cost-effectiveness and managerial efficiency. As a

[72]Cf. Brege *et al*., "Sourcing, insourcing and two times outsourcing".
[73]Goodman, "Infrastructure Goes Private", B1.
[74]Hyslop, *Critical information infrastructures* resilience, 5.
[75]Megginson and Netter, "From state to market", 380.
[76]Boin *et al., The Politics of Crisis Management*.

result, governments are reluctant to be the only party that is asked by the public to allocate necessary funds (and perhaps increase taxation for these purposes). Indeed, taking the cue from disaster recovery, Lee Miller *et al*. come to a conclusion that, by analogy, can substantially be applied to infrastructure development and protection: "Infrastructure upgrades that might sharply reduce [hurricane] Ike-type damages are excluded by cost-benefit analyses geared to maximize company and stockholder short-term interests."[77] It is the same conclusion that Ian Bartle and Marc Laperrouza reach, noting that because of liberalisation and internationalisation, particularly in Europe, CIIs are being operated well outside their original design parameters.[78]

Many, like John Dixon and Alexander Kouzmin, have cast doubts on the logic of "less state and less taxes",[79] which raises serious policy questions of social resilience and governance capacities in these diverse jurisdictions.[80] As observed by Petter Grytten Almklov and Stian Antonsen, "While the operation, maintenance and protection of critical infrastructures were traditionally seen as a public responsibility, the trend is now that this responsibility is transferred to the private sector or at least influenced by private-like modes of organizing."[81] More importantly, the corporatisation of CII, including the much lauded outsourcing, has in fact created more "responsibility gaps".

As Adam Smith theorised, safety and security have always been at odds with economic efficiency.[82] Societies should hence exercise great care in considering what conditions are necessary for protecting the public interest at a time when market forces exercise a lot of power.

In conclusion, in terms of security and accountability of outsourced CIIs, the "invisible hand" seems to be paralysed, while the eyes are cloudy and the ears seemingly deaf. This does not mean that the recent sudden post-crisis shift from outsourcing to insourcing will provide entirely secure systems. Coming close to achieving this is the best that can be striven for, in that it requires improved information-sharing before, during and after crises, and coordinated efforts to strengthen resilience in a reflexive and committed socio-technical fashion. Insourcing will however certainly help to clarify roles and responsibilities, something which is crucial for public accountability and, ultimately, for the safety and security of all.

Notes on Contributors

Lindy Newlove-Eriksson is Adjunct Lecturer at the Swedish Defence University (SEDU) and PhD Candidate at the Royal Institute of Technology (KTH), Stockholm, Sweden.

Giampiero Giacomello is Associate Professor of Political Science at the University of Bologna, Bologna, Italy. Email: Giampiero.giacomello@unibo.it

Johan Eriksson is Professor of Political Science at Södertörn University, Stockholm, Sweden. Email: johan.eriksson@sh.se

[77]Miller *et al*., "Hazards of neoliberalism", 512.
[78]Bartle and Laperrouza, "Systemic risk in network industries".
[79]Dixon and Kouzmin, "Public domains, organizations"; Kouzmin, "Market fundamentalism, delusions and epistemic failures".
[80]van Eeten and Bauer, "Emerging threats to internet security".
[81]Almklov and Antonsen, "The commoditization of societal safety", 133.
[82]See Bailes and Frommelt, *Business and security*.

ORCID

Lindy Newlove-Eriksson http://orcid.org/0000-0002-4249-4518
Giampiero Giacomello http://orcid.org/0000-0002-7053-9752
Johan Eriksson http://orcid.org/0000-0002-1526-0521

References

Abele-Wigert, I. "Challenges governments face in the field of critical information infrastructure protection (CIIP): Stakeholders and perspectives". In *International CIIP Handbook 2006, Vol. II: Analyzing issues, challenges, and prospects*, edited by M. Dunn and V. Mauer: 55–68. Zürich: Swiss Federal Institute of Technology, 2006.

Abele-Wigert, I., and M. Dunn, eds. *International CIIP handbook 2006 Vol I: An inventory of 20 national and 6 international critical information infrastructure protection policies.* Zürich: Swiss Federal Institute of Technology, 2006.

Almklov, P. G., and S. Antonsen. "The commoditization of societal safety". *Journal of Contingencies and Crisis Management* 18, no. 3 (2010): 132–44.

Anderson, C. "Swedish Government Scrambles to Contain Damage from Data Breach". *The New York Times*, 25 July 2017.

Andersson, J., and A. Malm. Public–private partnerships and the challenge of critical infrastructure protection. In *International CIIP handbook 2006, Vol. II: Analyzing issues, challenges, and prospects*, edited by M. Dunn and V. Mauer: 139–67. Zürich: Swiss Federal Institute of Technology, 2006.

Antonsen, S., P. G. Almklov, J. Fenstad and A. Nybø. "Reliability consequences of liberalization in the electricity sector: Existing research and remaining questions". *Journal of Contingencies and Crisis Management* 18, no. 4 (2010): 208–19. doi: https://doi.org/10.1111/j.1468-5973.2010.00619.

Bailes, A., and I. Frommelt, eds. *Business and security: Public-private sector relationships in a new security environment*. New York: Oxford University Press, 2004.

Bartle, I., and M. Laperrouza. "Systemic risk in the network industries: Is there a governance gap?". Paper presented at the 5th ECPR general conference, Potsdam University, 10 -12 September 2009.

Block, F., and M. R. Somers. *The Power of Market Fundamentalism: Karl Polanyi's critique*. Cambridge, MA: Harvard University Press, 2014.

Boin, A., P. t'Hart, B. Sundelius and E. Stern. *The Politics of Crisis Management*. Cambridge: Cambridge University Press, 2005.

Brege, S., P-O. Brehmer and H. Lindskog. "Sourcing, insourcing and two times outsourcing: four phases of procurement of telecommunications services within the Swedish public sector". *Strategic Outsourcing: An International Journal* 3, no. 2 (2010): 144–62.

Brendan, M. *In the Public Interest: Privatization and Public Sector Reform*. London: Zed Books Ltd, 1993.

Brevinge, N. "Regeringskrisen i juli 2017 i fyra delar" [The government crisis in four parts]. *Dagens Nyheter*, 29 July 2017.

Clifton, J., F. Comín and D. Fuentes. "Privatizing Public Enterprises in the European Union 1960–2002: Ideological, Pragmatic, Inevitable?" *Journal of European Public Policy* 13, no. 5 (2006): 736–56.

Cohen, F. "What makes critical infrastructures *critical*". *International Journal of Critical Infrastructures Protection* 3, no. 2 (2010).

Darab, A. "Statens Servicecenter varnade regeringen för outsourcing av it-drift" [The National Service Center warned the government about outsourcing IT management]. *Dagens Nyheter*, 24 July 2017.

de Brujine, M., and M. van Eeten. "Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment". *Journal of Contingencies and Crisis Managment* 15, no. 1 (2007): 18–29.

De la Reguera, E. "Sveriges statsminister Stefan Löfven om Transportstyrelsens it-skandal: En naivitet vad gäller outsourcing" [Sweden's prime minister Stefan Löfven about the Transport Agency's IT-scandal: a naivity about outcoursing]. *Dagens Nyheter*, 31 July 2017.

Delin, M. "IBM vägrar att svara på frågor om Sveriges regeringskris juli 2017" [IBM refuses to answer questions about Sweden's government crisis July 2017]. *Dagens Nyheter*, 27 July 2017.
Dixon, J., R. Dogan, and A. Kouzmin. "The dilemma of privatized public services: Philosophical frames in understanding failure and managing partnership terminations". *Public Organization Review* 4, no. 1 (2004): 25–46.
Dixon, J., and A. Kouzmin. "Public domains, organizations and neo-liberal economics: From de-regulation and privatization to the necessary 'smart state'". In *New Public Service*, edited by R. Koch, and P. Conrad: 263–91. Wiesbaden: Gabler Verlag/Springer, 2003.
Donahue, J. D. *The Privatization Decision: Public Ends, Private Means*. New York: Basic Books, 1989.
Dunn-Cavelty, M., and M. Suter. "The Art of CIIP Strategy: Taking Stock of Content and Process". In *Critical Infrastructure Protection: Advances in Critical Infrastructure*, edited by J. Lopez, R. Setola, and S. Wolfhusen. Berlin: Springer Verlag, 2012.
Dunn-Cavelty, M., and M. Suter. "Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection". *International Journal of Critical Infrastructure Protection* (2009): doi:https://doi.org/10.1016/j.ijcip.2009.08.006.
Ekdal, N. "It-läckaget på Transportstyrelsen är en symbol för den svenska aningslösheten" [The IT leakage at the Transport Agency is a symbol of Swedish naiveté]. *Dagens Nyheter*, 28 July 2017.
Eliner, M., and H. Jordahl. "Political preferences and public sector outsourcing". *European Journal of Political Economy* no. 30 (June 2013): 43–57.
European Council. "Council Directive 2008/114/EC of 8 December Identification and designation of European critical infrastructures". *Official Journal the European Union* 345/75, December 23, 2008. ww.scadahacker.com/library/Documents/Government/EU%20-%20European%20Critical%20Infrastructure.pdf.
Feigenbaum, H. B., and J. R. Henig. "The political underpinnings of privatization: A typology". *World Politics* 46, no. 2 (1994): 185–208.
Fitzgerald, R. *When Government Goes Private: Successful Alternatives to Public Services*. New York: Universe Books, 1988.
Fritzon, Å., K. Ljungkvist, A. Boin and M. Rhinard. "Protecting Europe's critical infrastructures: Problems and prospects". *Journal of Contingencies and Crisis Management* 15, no. 1 (2007): 30–41.
Goodman, P. S. "Infrastructure Goes Private And the Public Pays a Price". *The New York Times*, 16 June 2017, B1.
Goodman, J. B., and G. W. Lovemen. "Does privatization serve the public interest?" *Harvard Business Review* 69, no. 6 (1990): 26–8.
Green-Pedersen, C. "New Public Management reforms of the Danish and Swedish welfare states: The role of different Social Democratic Responses". *Governance* 15, no. 2 (2002): 271–94.
Griffin, A. "Sweden leaks details of almost all of its citizens in move that could bring down government". *The Independent*, 26 July 2017.
Grimsey, D., and M. Lewis. "Evaluating the risks of public private partnership for infrastructure projects". *International Journal of Project Management* 20, no. 2 (2002): 107–18.
Hall, P. "NPM in Sweden: The Risky Balance between Bureaucracy and Politics". In *Nordic Lights: Work, Entertainment and Welfare in Scandinavia*, edited by Å. Sandberg. Stockholm: SNS Publishing, 2013.
Hellström, T. "Critical infrastructure and systemic vulnerability: Towards a planning framework". *Safety Science* 45, no. 3 (2007): 415–30.
Henry, J. M. "The wave of privatization in the 1980s and 1990s: Was it inevitable?" Unpublished paper, 30 November 2006. http://ssrn.com/abstract=1293910, https://doi.org/10.2139/ssrn.1293910.
Hodge, G. A., and C. Greve. "Public–private partnerships: An international performance review". *Public Administration Review* 67, no. 3 (2007): 545–58.
Hoff, H. "KU-anmälning 2017/18:15 (105–2017/18) av Hans Hoff" [Report to the Constitutional Committee by MP Hans Hoff]. Stockholm: The Constitutional Committee of the Swedish Parliament, 2017.
Holmberg, K. "Läkarförbundet: Hanteringen av hälsointyg hot mot integriteten" [Swedish Medical Doctors Association: The handling of medical records is a threat to integrity]. *Dagens Nyheter*, 31 July 2017.

Hyslop, M. *Critical Information Infrastructures Resilience and Protection*. New York: Springer Science, 2007.
Jones, O. "Why Britain's Trains Don't Run on Time: Capitalism". *The New York Times*, 4 April 2017. https://www.nytimes.com/2017/04/04/opinion/why-britains-trains-dont-run-on-time-capitalism.html
Kallving, C-J. "Återföringen av it-driften till Sverige dröjer för Transportstyrelsen" [Insourcing of IT management to Sweden is delayed for the Transport Agency]. *Dagens Nyheter*, 28 July 2017.
Kaplan, F. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.
Kissel, R., ed. *Glossary of Key Information Security Terms*. NIST IR 7298 Revision 2. Washington DC: National Institute of Standards and Technology (NIST), US Department of Commerce, 2013. http://csrc.nist.gov/publications.
Kouzmin, A. "Market fundamentalism, delusions and epistemic failures in policy and administration". *Asia-Pacific Journal of Business Administration* 1, no. 1 (2009): 23–39.
Larsson, M. "Peter Hultqvists försvar: Vi har fullföljt vår del av ansvaret" [Peter Hultqvist's defence: We fulfilled our responsibilities]. *Dagens Nyheter*, 27 July 2017.
Larsson, D., and P. Qvist. "Säkerhetsexperterna Dan Larsson och Peder Qvist: 'Flera riksdagspartier bryter mot regler för it-säkerhet'" [Security experts Dan Larsson and Peder Qvist: Several parties in the Swedish parliament violate IT security regulations]. *Dagens Nyheter*, 1 August 2017.
Linder, S. H. "Coming to terms with the public-private partnership: A grammar of multiple meanings". *The American Behavioral Scientist* 43, no. 1 (1999): 35–51.
Lukasik, S. J., S. E. Goodman, and D. W. Longhurst. *Special Issue: Protecting Critical Infrastructures against Cyber-Attack*, Adelphi Paper 359. London: International Institute for Strategic Studies, 2003.
Megginson, W. L., and J. M. Netter. "From state to market: A survey of empirical studies on privatization". *Journal of Economic Literature* 39, no. 2 (2001): 321–89.
Metzger, J. "The concept of critical infrastructure protection". In *Business and Security Public-Private Sector Relationships in a New Security Environment*, edited by A. Bailes and I. Frommelt: 197–209. New York: Oxford University Press, 2004.
Miller, L., R. Antonio and A. Bonanno. "Hazards of neoliberalism: Delayed electric power restoration after hurricane Ike". *The British Journal of Sociology* 62, no. 3 (2011): 504–22.
Milne, R. "Sweden grapples with huge leak of confidential information". *Financial Times*, 24 July 2017.
Newland, S. J., and C. K. S Chun. *The European Campaign: Its Origins and Conduct*. Carlysle, PA: Strategic Studies Institute, US Army War College, 2011.
Örstadius, K. "Transportstyrelsens generaldirektör Maria Ågren nekar till brott"] [The Transport Agency's Director General Maria Ågren claims not guilty of crime]. *Dagens Nyheter*, 13 December 2017.
Örstadius, K. "Ågren sparkades – nu stäms staten" [Ågren was fired – now the government is sued]. *Dagens Nyheter*, 9 December 2017.
Örstadius, K. "Nya dokument från Maria Ågren: Transportstyrelsen pressades av Regeringskansliet" [New dopcuments from Maria Ågren: The Transport Agency was pressured by the government]. *Dagens Nyheter*, 31 August 2017.
Örstadius, K. "DN förklarar: It-skandalen på Transportstyrelsen – detta har hänt" [DN explains: The IT scandal at the Transport Agency – this is what happened]. *Dagens Nyheter*, 3 August 2017.
Örstadius, K. "Regeringskansliet lägger locket på om it-skandalen" [The government cover things up about the IT scandal]. *Dagens Nyheter*, 3 August 2017.
Örstadius, K. "Transportstyrelsens sparkade generaldirektör Maria Ågren röjde sekretessbelagda uppgifter som hotat rikets säkerhet" [The Transport Agency's fired Director General Maria Ågren revealed secret information that threatens national security]. *Dagens Nyheter*, 6 July 2017.
Palm, J. "Emergency management in the Swedish electricity market: The need to challenge the responsibility gap". *Energy Policy* 36, no. 2 (2008): 843–9.
Perrow, C. *Normal Accidents: Living with High Risk Technologies*. Princeton: Princeton University Press, 1999.
Pescaroli, G., and D. Alexander. "Critical infrastructures, panarchies and the vulnerability path of cascading disasters". *Natural Hazards* 82, no. 1 (2016): 175–92.
Pirie, M. *Privatization: Theory, Practice and Choice*. Aldershot: Wildwood House Limited, 1988.

Plietzch, A., P. Schultz, J. Heitzig and J. Kurths. "Local vs global redundancy – trade-offs between resilience against cascading failures and frequency stability". *The European Physical Journal Special Topics* no. 225 (2016): 551–68.
Porter, E. "When Public Outperforms Private in Services". *The New York Times*, 16 January 2013, B1.
Qviberg, T. "It-kompetensen är obefintlig på svenska myndigheter" [IT competence is nonexistent in Swedish public agencies]. *Dagens Nyheter*, 31 July 2017.
Redenius, C. "The supply-side alternative: Reagan and Thatcher's economic policies". *The Journal of Social, Political, and Economic Studies* 8, no. 2 (1983): 189–209.
Riksrevisionen (National Audit Office). "IT inom statsförvaltningen – har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?" [IT within the state administration - have the authorities tried in a reasonable manner to ask whether outsourcing contributes to enhanced efficiency?]. *Riksrevisionen*, RiR 2011, 4. https://www.riksrevisionen.se/PageFiles/8528/Anpassad_11_4_IT%20inom%20statsf%C3%B6rvaltningen.pdf.
Ryu, D. H., H. Kim and K. Um. "Reducing security vulnerabilities for critical infrastructure". *Journal of Loss Prevention in the Process Industries* 22, no. 6 (2009): 1020–4.
Savas, E. S. *Privatization: The Key to Better Government*. New Jersey: Chatham House Publishers, 1987.
Sheil, C. *Water's Fall: Running the Risks with Economic Rationalism*. Annadale, NSW: Pluto Press Australia, 2000.
Svahn, C. "Säpos tillsyn avslöjade brottet" [Säpo's review revealed the crime]. *Dagens Nyheter*, 6 July 2017.
Swedish Transport Agency, *Kartlägga hanteringen av vissa uppgifter: rapport till regeringen* [Mapping the handling of certain information: report to the government]. Official report from the Transport Agency no. TSG 2017-2515. Stockholm, 23 January 2018. https://www.transportstyrelsen.se/globalassets/kartlagga-hanteringen-av-vissa-uppgifter.pdf
van Eeten, M., and J. M. Bauer. "Emerging threats to internet security: Incentives, externalities and policy implications". *Journal of Contingencies and Crisis Management* 17, no. 4 (2009): 222–32.
Vickers, J., and V. Wright. "The politics of industrial privatization in Western Europe: An overview". *West European Politics* 11, no. 4 (1988): 1–30.
Wilhelmson, A. "S-ledamoten Hans Hoff KU-anmäler förra regeringen" [Social Democratic MP Hans Hoff reports the former government to the Constitutional Committee for investigation]. *Dagens Nyheter*, 27 July 2017.
Wolfe, J. "State power and ideology in Britain: Mrs Thatcher's privatization program". *Political Studies* 39, no. 2 (1991): 237–52. doi:https://doi.org/10.1111/j.1467-9248.1991.tb01365.