Crime Terror
Nexus

Public-Private Partnership in Security: Lessons from Banking, Cyber, and Infrastructure

1 Introduction[1]

In 2017, the UN Security Council passed resolution 2341, which called for member states to share information in order to protect critical infrastructure from terrorist attacks.[2] Addressing the Security Council, Hamid Ali Rao, Deputy Director General of the Organisation for the Prohibition of Chemical Weapons (OPCW), said that this responsibility must be shared equally by industry and government.[3] His sentiments were echoed by many other speakers, who emphasised the key role of public-private partnerships (PPPs). But what are PPPs? And why are they important?

In the 1980s and 1990s, key public utilities began to be outsourced to the private sector in what became known as a "privatization wave".[4] After the September 11, 2001 attacks on the United Sates, it was found that 85% of critical infrastructure was controlled by private actors.[5] Today, the vast majority of critical infrastructure assets around the world are privately owned and the private sector is responsible for their protection.[6]

Involving the private sector in providing security is not only sensible, therefore, but inevitable.[7] Whereas the state remains the main provider of security, it can only guarantee this by collaborating with private actors in the execution of its responsibility, as in many instances they are the first target and first responders to attacks.

But the utility of PPPs goes far beyond the specific example of critical infrastructure. What makes PPPs unique is the ability to draw on both the public and private sectors to provide goods and services, which cannot be delivered by individual organisations (be they public or private) on their own.[8] Together, they aim to ease public sector budgetary constraints while simultaneously delivering a more efficient outcome.[9] As the European Commission points out, PPPs have the potential to "make the best use

1 The authors of this report are Zora Hauser and Devorah Margolin. We are grateful to all interviewees, whether named or anonymous.
2 The United Nations (2017) "Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017)". https://www.un.org/press/en/2017/sc12714.doc.htm
3 The United Nations (2017) "Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017)". https://www.un.org/press/en/2017/sc12714.doc.htm
4 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
5 The 9/11 Commission Report. (2002) http://govinfo.library.unt.edu/911/report/911Report.pdf
6 The United Nations (2018) "The protection of critical infrastructures against terrorist attacks: Compendium of good practices". https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf
7 Interview with Stefano Betti, Deputy Director General, Transnational Alliance to Combat Illicit Trade. April 25, 2019. London.
8 Hans Van Ham & Joop Koppenjan (2001) "Building Public-Private Partnerships: Assessing and managing risks in port development", Public Management Review, 3:4, 593-616
9 European Court of Auditors (2018) "Public Private Partnerships in the EU: Widespread shortcomings and limited benefits" https://www.eca.europa.eu/Lists/ECADocuments/SR18_09/SR_PPP_EN.pdf

of private sector operational efficiencies to reduce cost and increase quality to the public".[10]

Today, there are hundreds of academic articles and policy papers focusing on public-private partnerships, yet a clear understanding of the concept is lacking, as PPP arrangements come in many forms and have been championed by both public and private parties. Over time, they have proved to fail as often as they succeed.[11]

This paper will look at three European case studies in the areas of banking, cyber, and infrastructure. In doing so, it aims to showcase a variety of PPP programmes that have already been implemented in the field, examine their structures, and assess the ways in which they have operated.

These case studies are:

- the Joint Money Laundering Intelligence Taskforce (JMLIT) in the United Kingdom;
- the Cyber Security Council in the Netherlands;
- the International Airport in Hamburg, Germany.

Each highlights different relationships between the public and private sectors. While all three of these relationships are contractual, some will prove to constitute more pragmatic and mutually beneficial relationships than others. The study of existing PPPs that deal with current security issues are vital as we seek to understand their successes and failures and taking lessons learned to explore the potential of future collaboration.

The report shows that public-private partnership can create win-win situations if they are strategic, if interests are mutual and expectations are realistic. The different examples illustrate that one size does not fit all, and that partnerships need to take into account specific national and sector-specific circumstances. They also show that partners need to be flexible, and adjust their expectations according to changing situations. Most importantly, they demonstrate that much is to be gained if public and private sectors generate trust, make genuine attempts to understand each other's perspectives, and develop protocols for dealing with areas of common interest.

10 Guidelines for successful Public–Private Partnerships" European Commission. 2003. https://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf

11 Graeme A. Hodge, Carsten Greve, and Anthony Boardman (2010). International handbook on public-private partnerships. Edward Elgar Publishing.; Roger Wettenhall (2005). The public-private interface: surveying the history. *The challenge of public-private partnerships: Learning from international experience*, 22-43.; Roger Wettenhall (2003). The rhetoric and reality of public-private partnerships. *Public Organization Review*, 3(1), 77-107.

2 What are PPPs

Despite the popularity of the term, there continues to be widespread confusion over what constitutes a public private partnership (PPP).[12] At the same time, many European and international organisations, alongside the academic community, have made efforts to systematically describe the content, mechanisms, and nature of such a relationship.

The Organisation for Economic Co-operation and Development (OECD) has emphasised the necessity of coordination with the private sector,[13] especially in the field of critical infrastructure.[14] It offers a broad understanding of PPPs, and defines it as "long term contractual arrangements between the government and a private partner whereby the latter delivers and funds public services using a capital asset, sharing the associated risks".[15]

Despite the specificity of such definitions, the terms contractual partnership and public-private partnership are often used interchangeably.[16] Some authors have tried to address this point, for example by providing a differentiation between "traditional PPPs" and so-called "Private Finance Initiatives (PFIs)", which exclusively focus on private sector money for infrastructure projects that are paid off over time by the public sector.[17]

A slightly narrower definition is provided by the European Investment Bank, which states that PPPs are relationships that are (1) initiated by the public sector; (2) must involve a clearly defined project for the parties involved to complete; (3) must have a time-limited contractual relationship (in other words, they cannot be indefinite); (4) have shared risk taking between the public and private sectors; and (5) have a clear separation between the public and private actors.[18]

12 Robert Brain (2009) "Review of Lessons from Completed PPP Projects Financed by the EIB" European Investment Bank. https://bankwatch.org/sites/default/files/EIB-PPP-review.pdf
13 OECD (2013) "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace" https://www.osce.org/atu/103500?download=true
14 OECD (2008) "OECD Recommendation of the Council on the Protection of Critical Information Infrastructure" http://www.oecd.org/sti/40825404.pdf
15 OECD (2012) "Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships" https://www.oecd.org/governance/budgeting/PPP-Recommendation.pdf
16 Graeme A. Hodge and Carsten Greve (2007). "Public-Private Partnerships: An International Performance Review." *Public Administration Review* 67(3): 545-558.
17 UK Parliament (2011) "Public Accounts Committee – Forty-Fourth Report Lessons from PFI and other projects" https://publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1201/120102.htm
18 European Investment Bank (2005) "Evaluation of PPP projects financed by the EIB" http://www.eib.org/attachments/ev/ev_ppp_en.pdf

Other efforts have aimed at defining the specific role of the private sector in PPP schemes. For example, according to the European Commission, private actors should bring to the table: (1) additional capital; (2) alternative management and implementation skills; (3) value added to the consumer and the public at large; and (4) better identification of needs and optimal use of resources.[19]

By contrast, Hodge and Greve have distilled the many different understandings and discussions around public-private partnerships into three key components of this specific form of collaboration: (1) the sturdiness of the relationship (it cannot be short-term); (2) the sharing of risk; and (3) the joint production of a product or service with mutual gain.[20]

While comparing such definitions might offer useful insight, it is equally important to consider practical examples, which will we focus on for the main part of this report.

19 Guidelines for successful Public–Private Partnerships" European Commission. 2003. https://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf

20 Graeme A. Hodge and Carsten Greve (2007). "Public-Private Partnerships: An International Performance Review." *Public Administration Review* 67(3): 545-558.

3 What is a Successful PPP?

While everyone likes to talk about public-private partnerships, their implementation can be challenging. According to Stefano Betti, Deputy Director General of Transnational Alliance to Combat Illicit Trade:

> *There is a mismatch between what people say at conferences all around the world about the absolute need to have these partnerships, and the reality on the ground, which shows that it is not so easy to form these partnerships. And when they are formed they are not so easy to maintain and to sustain.*[21]

Though often vague,[22] guidelines and instructions for successful relationships between the public and private sectors are plentiful. According to the United Nations, for example, successful PPPs: (1) appreciate success and constraint factors; (2) define their scope; (3) define their forms; and (4) anticipate problems and challenges".[23] Failures, by contrast are rooted in "expectation gaps between the private and the public sector, unsustainable funding models, [and] unclear divisions of labor".[24]

For the European Commission, success is determined by four conditions: (1) "ensuring open market access and fair competition; (2) protecting the public interest and maximising value added; (3) defining the optimal level of grant financing both to realise a viable and sustainable project but also to avoid any opportunity for windfall profits from grants; [and (4)] assessing the most effective type of PPP for a given project."[25]

In 2013, the Organization for Security and Co-operation in Europe (OSCE) created a guide for how European countries could maximise the benefits of a public-private partnership.[26] It argued that the following eight considerations were key in identifying and leveraging common interests: (1) identifying the motivations for joining the PPP; (2) defining the overall goals of the PPP and the purpose of the partnership; (3) understanding and abiding by the regulatory framework; (4) providing mechanisms for information sharing; (5) clarifying the roles of the public and private actors involved; (6) starting small and growing steadily; (7) identifying milestones; and (8) constantly reviewing the process to continue to strengthen the partnership.

21 Interview with Stefano Betti, Deputy Director General, Transnational Alliance to Combat Illicit Trade. April 25, 2019. London.
22 Guidelines for successful Public–Private Partnerships" European Commission. 2003. https://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf
23 The United Nations (2018) "The protection of critical infrastructures against terrorist attacks: Compendium of good practices". https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf
24 The protection of critical infrastructures against terrorist attacks: Compendium of good practices. The United Nations (2018) https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf
25 Guidelines for successful Public–Private Partnerships" European Commission. 2003. https://ec.europa.eu/regional_policy/sources/docgener/guides/ppp_en.pdf
26 OSCE (2013) "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace". Pg. 69 https://www.osce.org/secretariat/103500?download=true

4 A History of PPPs in Security

Before introducing the case studies, it might be useful to consider the history – and specific challenges – of public-private partnerships in the field of security.

Early examinations of phenomenon of PPPs in the 1960s and 1970s mostly focused on infrastructure, such as hospitals and social welfare programmes.[27] In the 1980s and 1990s, key public utilities, such as critical information infrastructures, began to be outsourced to the private sector.[28] This made it inevitable to include private actors in governance conversations,[29] resulting in a wave of literature focusing on public-private partnerships in infrastructure security.[30] More specifically, research began to look at PPP's in the prison system,[31] partnerships to fight corruption,[32] as well as crime-fighting, public safety[33] and technology.[34]

However, according to Wettenhall, the scholarly debate surrounding public-private partnerships only began to develop in the early 2000s.[35] Up to this period, it was found that most PPPs were in fact transactional contracts.[36] With the rise of PPP discussions in the financial sector and the adoption by the UK government of the Private Finance Initiative, later rebranded as public-private partnerships,[37] a new wave of literature on public-private partnership programmes – focusing on their promotion, as well as the challenges involved in their successful implementation – emerged.[38]

27 Charles A. Reich, (1965). Social Welfare in the Public-Private State. U. Pa. L. Rev.; Ronald P. Burd and Julius B. Richmond. (1979) "The public and private sector: A developing partnership in human services." American Journal of Orthopsychiatry 49(2); David Kopelman (1969). Public-Private Partnership: Its Impact upon Hospitals and Related Health-Care Institutions: Discussions. *Bulletin of the New York Academy of Medicine*, *45*(11).; William S Tennant et al. (1979) "Financing Housing and Urban Renewal Projects." *The Urban Lawyer*: 416-434.

28 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

29 Institute on Governance, Suzanne Taschereau, José Edgardo L. Campos, and International Conference on Governance Innovations (1996: Manila, Philippines). *Governance Innovations: Lessons from Experience: Building Government-citizen-business Partnerships*. Institute on Governance.

30 Edith M. Van den Berg (1995). Crime prevention on industrial sites: Security through public-private partnerships. *Security Journal*, *6*(1), 27-35.; Ginger Smith (1999). Toward a United States policy on traveler safety and security: 1980-2000. *Journal of Travel Research*, *38*(1).

31 Travis Pratt & Jeff Maahs, (1999). Are private prisons more cost-effective than public prisons? A meta-analysis of evaluation research studies. *Crime & Delinquency*, *45*(3), 358-371.; Anne L. Schneider (1999). Public-private partnerships in the US prison system. *American Behavioral Scientist*, *43*(1), 192-208.

32 Klitgaard, Robert and Heather Baser, (1998) Working together to fight corruption: state, society and the private sector in partnership. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/reprints/RP693.html. Also available in print form.

33 David Vidaver-Cohen (1998). Public–Private Partnership as a Strategy for Crime Control: Corporate Citizenship Makes the Difference. *Business and society review*, *100*(1), 21-31.; Meredith Whiting (1999). Innovative public-private partnerships: Public safety initiatives. Conference Board.

34 Joseph Stiglitz & Scott Wallsten (1999). Public-Private Technology Partnerships: Promises and Pitfalls. *American Behavioral Scientist*, 43(1), 52–73. https://doi.org/10.1177/00027649921955155

35 Roger Wettenhall (2003). The rhetoric and reality of public-private partnerships. *Public Organization Review*, *3*(1), 77-107.

36 Tony Bovaird, (2004). Public–private partnerships: from contested concepts to prevalent practice. International review of administrative sciences, 70(2), 199-215.

37 Michael G. Pollitt (2005). Chapter 11. Learning from UK private finance initiative experience. In *The Challenge of public-private partnerships: Learning from International Experience* edited by Graeme A. Hodge, Carsten Greve

38 Graeme Hodge & Carsten Greve (Eds.). (2005). *The challenge of public-private partnerships: Learning from international experience*. Edward Elgar Publishing.; Jane Broadbent & Richard Laughlin (2003). Public private partnerships: an introduction. Accounting, Auditing & Accountability Journal, 16(3), 332-341.; Erik-Hans Klijn and Geert R. Teisman. (2003) "Institutional and strategic barriers to public—private partnership: An analysis of Dutch cases." *Public money and Management* 23(3): 137-146.

It was also at this time that analysts and experts started looking at public-private partnerships in the field of security. Much of the early literature on private sector contributions to security focused on for profit private actors, such as private military companies.[39] More recently, researchers and policy makers have started to explore the roles that private actors can play in countering terrorism. For example, Bures conducted a study titled "Public-private partnerships in the fight against terrorism?" in 2013 in which he addressed the lack of academic literature but acknowledged the many roles that private actors have played in protecting physical infrastructure. He argued that there was a widespread lack of appreciation for the roles that private actors have played in counter-terrorism – "both willingly an unwillingly".[40]

His work built on the research of others, including Petersen's "Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility?" in which he argued that the private sector could play a role in counter-terrorism, but that risk considerations of private companies were not always compatible with national security interests.[41]

In an interview with the authors, Bures added that the main issue with many PPP's is the clear differences in priorities between the private actors and public actors, noting "there is a big difference in the motivations for the public and private sectors. For the public sector, costs are secondary concern, while for the private sector, they are interested in profit maximizing."[42] Although their interests regarding security do overlap with the public interests, public partners must acknowledge private partners strategic goals.[43]

39 Patrick Cullen (2000). Keeping the new dog of war on a tight leash. Assessing means of accountability for private military companies. Conflict Trends, 2000(1), 36-39.; Bures, Oldrich. (2013) "Public-private partnerships in the fight against terrorism?" Crime, law and social change 60, no. 4: 429-455.

40 Oldrich Bures (2013) "Public-private partnerships in the fight against terrorism?" Crime, law and social change 60, no. 4: 429-455.

41 Karen Lund Petersen (2008) "Risk, responsibility and roles redefined: is counterterrorism a corporate responsibility?" *Cambridge Review of International Affairs* 21, no. 3: 403-420.

42 Interview with Oldrich Bures, Professor, Metropolitan University Prague. May 9, 2019. London.

43 Oldrich Bures (2013). "Public-private partnerships in the fight against terrorism?" Crime, law and social change 60, no. 4: 429-455

5 Case Studies

The issues that have been brought up in the literature regarding the risk, as well as the role and untapped potential for private actor participation, still ring true today. This paper looks at three European case studies in the areas of banking, cyber security, and infrastructure. Each of them highlights different relationships between the public and private sectors. By doing so, this paper aims to showcase a variety of PPP programs that have already been implemented in the field of security, as well as examine their structures and ways of operating.

Case Study 1 – Banking

Background

According to an estimate by Transparency International, transnational organised crime generated income equivalent to around 2.7% of global GDP in 2017, with approximately $1.6 trillion laundered to disguise its criminal origins.[44] Since September 11, 2001, stopping the flow of illicit financial flows has become one of the key activities to counter international terrorism.[45]

The two main areas driving counter terrorism financing have come from the United Nations Security Council sanctions model and the Financial Action Task Force (FATF) anti-money laundering activities. The UN model focuses on the "United Nations Security Council Consolidated List", a list of individuals and entities sanctioned by the Security Council.[46] On the other hand, the G-7's Financial Action Task Force (FATF) model is built around the *Forty Recommendations for pursuing the fight against money laundering* and *Nine Special Recommendations*, which have now become the international standard for fighting terrorism.[47]

This section will examine the Joint Money Laundering Intelligence Taskforce (JMLIT) that was launched by the British government. Its success has triggered other public-private financial information-sharing partnership in Australia, Singapore, Hong Kong, as well as the US and Canada, all modelled after the UK experience.[48] While private-public partnerships

44 Chris Price (2017) "Cleaning up: Britain is taking on the money launderers". The Telegraph. https://www.telegraph.co.uk/technology/britain-takes-on-money-launderers/
45 Oldrich Bures (2013) "Public-private partnerships in the fight against terrorism?" Crime, law and social change 60, no. 4: 429-455.
46 'United Nations Security Council Consolidated List' https://www.un.org/securitycouncil/content/un-sc-consolidated-list
47 International Standards on Combating Money Laundering in the Financing of Terrorism & Proliferation: The FATF Recommendations (updated 2018) http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
48 Tom Keatinge (2017) "Public–Private Partnerships and Financial Crime: Advancing an Inclusive Model" RUSI. https://rusi.org/commentary/public%E2%80%93private-partnerships-and-financial-crime-advancing-inclusive-model

in the financial sector have become more prevalent, they are still considered relatively new as an approach to stopping financial crimes.[49]

Joint Money Laundering Intelligence Taskforce (JMLIT): How does it work?

As a financial hub, the UK is a prime target for money laundering. According to the UK National Risk Assessment on Money Laundering & Terrorist Financing, £100 billion annually is laundered through the UK.[50]

In response to this threat, and in compliance with international and European guidelines, The Joint Money Laundering Intelligence Taskforce (JMLIT) was launched by the UK government as an initiative between the financial sector and security agencies in order to combat money laundering and financial crimes. JMLIT is a public-private financial information-sharing partnership (FISP), which brings together law enforcement, other public sector agencies and financial institutions to help tackle money laundering and financial crimes. Beyond information and intelligence sharing, the JMLIT works to create products to increase private sector understanding of risks connected to financial crime, and their implications.

Initiated in 2015, and established permanently in May 2016, public and private partners in JMLIT include:

- Law enforcement (tax authorities, City of London Police, Metropolitan Police Service);
- Other Government agencies (national crime agencies, Serious Fraud Office, and fraud prevention service);
- The British Bankers Association, alongside more than 40 UK and international banks, including Barclays, BNP Paribas, Citigroup, Deutsche Bank, JP Morgan, HSBC, Lloyds, Metro Bank, Nationwide, Post Office, RBS, Santander and Standard Chartered.

All the actors are coordinated and led by a taskforce, or management board, which reports on JMLIT's activities to the Financial Sector Forum, which is made up of senior representatives from government, regulation, and banking.[51]

Currently, the objectives of the JMLIT are:[52]

1. Understanding and disrupting the funding flows linked to bribery and corruption;
2. Understanding and disrupting trade-based money laundering;

49 Nick J Maxwell and David Artingstall (2017) "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime" RUSI. https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwwell_artingstall_web_4.2.pdf

50 National Crime Agency (2018) "National Crime Agency Annual Report and Accounts 2017–18". http://nationalcrimeagency.gov.uk/publications/915-nca-annual-report-account-2017-18/file

51 Joint Money Laundering Intelligence Taskforce (JMLIT). http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-economic-crime-centre/joint-money-laundering-intelligence-taskforce-jmlit

52 Joint Money Laundering Intelligence Taskforce (JMLIT). http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-economic-crime-centre/joint-money-laundering-intelligence-taskforce-jmlit

3. Understanding and disrupting the funding flows linked to organised immigration crime, human trafficking and modern slavery
4. Understanding and disrupting money laundering through capital markets; and
5. Understanding key terrorist financing methodologies.

How is the JMLIT unique?

The work of JMLIT has in only one year, between May 2016 and March 2017, led to the arrest of 63 individuals suspected of money laundering, as well as 1,000 bank-led investigations into financial crime.[53] In addition, the JMLIT was able to identify more than 2,000 accounts previously unknown to law enforcement, closed more than 450 bank accounts suspected of being used for money laundering, heightened monitoring of more than 400 accounts; granted more than 40 Proceeds of Crime Act orders, as well as produced 19 alerts and one strategic assessment on money laundering typologies.[54] According to the FATF, since 2015, JMLIT's work has led to 105 arrests, but seized only approximately £9 million in funds. [55]

Beyond such quantitative results, JMLIT experts have also focused on gaining a qualitative understanding of the phenomenon of financial crime. As it recognised itself, one of the greatest contributions has been "an improved collecting understanding of new and emerging money laundering threats" and the "targeted and coordinated interventions by law enforcement and the financial sector", as well as the use of "tools and expertise across the public and private sector to tackle money laundering threats impacting the UK." [56]

One key aspect that differentiates the JMLIT from other FISPs is in fact its collaborative and voluntary nature. While situated within the existing legislation, the fact that banks have a voice in the development of the policies should be seen as a success and a step in the right direction towards a more collaborative effort. According to former Prime Minister Theresa May, banks in the UK are

> *… not doing it because they have been forced to by a regulator. This is entirely voluntary; there is no regulatory or legal requirement to do it, although it will operate fully within existing legislation. The banks are committed to this work because making the UK's financial sector even more hostile to criminals is clearly as much a priority for them as it is for government and law enforcements agencies.*[57]

53 Chris Price (2017) "Cleaning up: Britain is taking on the money launderers". The Telegraph. https://www.telegraph.co.uk/technology/britain-takes-on-money-launderers/
54 Joint Money Laundering Intelligence Taskforce (JMLIT). http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-economic-crime-centre/joint-money-laundering-intelligence-taskforce-jmlit
55 FATF (2018) "Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report" http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf
56 Joint Money Laundering Intelligence Taskforce (JMLIT). http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-economic-crime-centre/joint-money-laundering-intelligence-taskforce-jmlit
57 The Rt Hon Theresa May MP (2015) "Theresa May announces launch of Joint Money Laundering Intelligence Taskforce". The Home Office. https://www.gov.uk/government/speeches/home-secretary-on-the-work-of-the-financial-sector-forum

Assessment

Despite the relatively small amount of money seized, JMLIT is widely seen as a success by the UK and the international financial community, as it has addressed some of the key problems in public-private sector collaboration in the financial sector.[58]

One of those challenges is over-reporting. Due to the heavy penalties for non-compliance and reputational risks, most financial institutions tend to over-report so-called suspicious activities (SAR) to the authorities,[59] resulting in a completely unbalanced flow of information.[60] While law enforcement agencies are only able to share limited information with the private sector, approximately 80-90% of reports coming from the private sector on suspicious financial activity do not provide operational value to law enforcement.[61] According to Europol, of the one million SARs filed annually, only about 10% are investigated by law enforcement.[62] Most participants agree that the JMLIT has increased the quality of the SAR reporting, lowering the number of "cry wolf" reports. While this has been limited to the larger institutions involved in the project and has worked best for high priority cases,[63] it has had an impact on the entire banking sector, including non-JMLIT banks, who have adopted suspicious activity reporting based on the JMLIT created alerts.[64] Further improvements are expected, as private sector companies are working to create more advanced machine learning that can detect criminal activities without over flagging cases.[65]

JMLIT is also credited with improving the speed of reporting on financial crimes in the UK. Maxwell and Artingstall argue that in the UK, "the speed of the response to major terrorist incidents in 2017 appears to have been significantly improved by the UK's financial information-sharing partnership".[66] In its December 2018 report of the UK, the FATF praised the UK's JMLIT information sharing PPP programme, labelling JMLIT as "an example of best practice". [67] Specifically, the FATF highlighted the JMLIT's sharing of information, that went beyond mandatory AML reporting, worked on active investigations, and identified future threats.

58 For example, see: Georges Favarel-Garrigues, Thierry Godefroy, and Pierre Lascoumes (2011). Reluctant partners? Banks in the fight against money laundering and terrorism financing in France. Security Dialogue, 42(2), 179–196.; Oliver Hart (2003). Incomplete contracts and public ownership: Remarks, and an application to public-private partnerships. *The Economic Journal*, 113(486), C69-C76.; Eric-Hans Klijn and Geert R. Teisman (2000) "Governing public-private partnerships." *Public-Private Partnerships, Theory and Practice in International Perspective* 180.; Myriam Dunn-Cavelty and Manuel Suter (2009) "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection* 2(4): 179-187.

59 Oldrich Bures (2013). "Public-private partnerships in the fight against terrorism?" Crime, law and social change 60, no. 4: 429-455

60 Előd Takáts (2007) "A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement" International Monetary Fund Working Paper. https://www.imf.org/external/pubs/ft/wp/2007/wp0781.pdf

61 Nick J Maxwell and David Artingstall. (2017) "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime" RUSI. https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_4.2.pdf

62 Chris Price (2017) "Cleaning up: Britain is taking on the money launderers". The Telegraph. https://www.telegraph.co.uk/technology/britain-takes-on-money-launderers/

63 FATF (2018) "Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report" http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf

64 FATF (2018) "Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report" http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf

65 Chris Price (2017) "Cleaning up: Britain is taking on the money launderers". The Telegraph. https://www.telegraph.co.uk/technology/britain-takes-on-money-launderers/

66 Nick J Maxwell and David Artingstall (2017) "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime" RUSI. https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_4.2.pdf

67 FATF (2018) "Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report" http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf

Lastly, banks have benefited from government briefings, for example on the designations of terrorist actors. Using such information, they have been able to make sure that terrorist individuals cannot operate or hold bank accounts, and respond to designations earlier and with more accuracy.[68]

Despite such improvements, former banker and financial security specialist Tom Keatinge argued that the relationship between the two parties could still be developed, and that its aim should be to become as comprehensive, far-ranging and systemic as possible. He said:

> *I think you have to think very carefully about what you are trying to achieve with the partnership. Because the partnership is not the be all and end all. The partnership should be part of a reengineering of the system that reflects modern technology, modern data gathering techniques, modern monitoring techniques, and uses the FinTech tools that are developing.*[69]

Case Study 2 – Cyber

Background

International cyber security policy has traditionally been driven by the United States. Built on the belief that private actors had the skills necessary to address these issues, while acknowledging the gaps in the public sector,[70] US policies were the first to push the private sector to take a leading role in cyber-security,[71] and still today constitute the "cornerstone" on which many other countries have modelled their policies.

More recently, the European Union has started to develop its own set of policies and initiatives responding to cyber threats and involving both public and private actors. In 2013, the EU Cyber Security Strategy was designed with the intent to provide a safe and free-access cyberspace.[72] Three years later, the first piece of EU-wide legislation on cybersecurity – the Directive on Security of Network and Information Systems (NIS Directive) – was adopted.[73] Other European initiatives include the European Union Agency for Network and Information Security (ENISA) and the PPP between the European Commission and, the cyber security sector, represented by the European Cyber Security Organisation (ECSO)[74].

68 Interview with Tom Keatinge, Director of the Centre for Financial Crime and Security Studies, RUSI. April 26, 2019. London.
69 Interview with Tom Keatinge, Director of the Centre for Financial Crime and Security Studies, RUSI. April 26, 2019. London.
70 Raphael Bossong and Ben Wagner. (2017) "A typology of cybersecurity and public-private partnerships in the context of the EU." Crime, Law and Social Change 67(3): 265-288.
71 Joseph Stiglitz & Scott Wallsten (1999). Public-Private Technology Partnerships: Promises and Pitfalls. *American Behavioral Scientist*, 43(1), 52–73. https://doi.org/10.1177/00027649921955155
72 European Commission "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace" February 2013 https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace
73 European Commission. "The Directive on security of network and information systems (NIS Directive)" https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
74 The European Union Agency for Network and Information Security (ENISA) https://www.enisa.europa.eu/; European Commission "Commission signs agreement with cybersecurity industry to increase measures to address cyber threats" July 2016 https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-cybersecurity-industry-increase-measures-address-cyber-threats

The Netherlands is recognised among the 10 most digitally savvy countries in the world[75] and ranks fourth of the 28 member states for the most advanced digital economies.[76] As approximately 80% of critical processes in the digital arena are in the hands of private parties,[77] public-private cooperation forms the backbone of the Dutch approach to cybersecurity.[78] This section will explore how this works in practice.

Cyber Security Council in Netherland: How does it work?

The Dutch cybersecurity policy is driven by the National Cyber Security Agenda, which promotes knowledge sharing – between the public and private sectors, but also the EU and NATO – as a crucial ingredient to the development of cyber security policies and their execution.[79] Within this framework, in 2011, the Cyber Security Council (CSR), an independent body made up of members from the public and private sector who advise the Dutch Cabinet on matters of cyber security, was created.[80]

The Cyber Security Council has three main functions:[81]

- Providing solicited and unsolicited strategic advice on cyber security to the Dutch government and the business community (through the government);
- Monitoring trends and new technological developments and, where necessary, translating these into potential measures to reduce the cyber security risks and to increase the economic opportunities;
- Initiating and/or accelerating relevant initiatives in the Netherlands and in the European Union that demonstrably contribute to raising the level of cyber security in the Netherlands.

While founded by a government subsidy, the CSR aims at providing the private sector with an equal voice to the public sector.[82] Of a total of 18 members, seven come from the private sector, seven come from the public sector, and four are from the scientific community.

- Private Sector Members represent leading companies in the Netherlands, with a particular focus on those engaged in the cyber and security areas.
- Public Sector Members include representatives of the armed forces, the Ministry of the Interior, the Ministry of Economic Affairs, the intelligence services and the police.
- Scientific Community Members are academics in cyber-related areas at leading Dutch universities.

75 Jurica Dujmovic (2016) “The 10 most digitally savvy countries in the world” Market Watch. https://www.marketwatch.com/story/the-10-most-digitally-savvy-countries-in-the-world-2016-07-19
76 “The Digital Economy and Society Index (DESI)” (2018). https://ec.europa.eu/digital-single-market/en/desi
77 “ Resilient critical infrastructure” National Coordinator for Security and Counterterrorism Ministry of Justice and Security. (2018) https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf
78 “National Cyber Security Agenda: A cyber secure Netherlands” NCTV. (2018) https://english.nctv.nl/binaries/CSAgenda_EN_def_web_tcm32-339827.pdf
79 “National Cyber Security Agenda: A cyber secure Netherlands” NCTV. (2018) https://english.nctv.nl/binaries/CSAgenda_EN_def_web_tcm32-339827.pdf
80 Melissa Hathaway and Francesca Spidalieri. (2017) “The Netherlands Cyber Readiness at a Glance.” Potomac Institute for Policy Studies, May 2017. http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf
81 Dutch Cyber Security Council https://www.cybersecurityraad.nl/index-english.aspx
82 “Public Private Partnerships (PPP) Cooperative models” (2017) European Union Agency For Network and Information Security

Rather than one chair, the CSR has two co-chairs, one from the public sector and one from the private sector.[83] The government co-chair on the CSR is the National Coordinator for Security and Counterterrorism[84]

How is the Cyber Security Council unique?

The Cyber Security Council (CSR) has no operational role, but functions as an independent advisor to the government.[85] It regularly meets and produces publications and advisory documents, such as the CRS Annual Magazine and Annual Report, alongside commissioning research projects, running conferences, and even a cyber security summer school.[86]

Each year, the CSR focuses on a number of forward-looking themes which address societal and economic issues related to strengthening cyber security in the Netherlands. For example, in 2017, the CSR focused on issues related to "duties of care", that is, a duty to ensure adequate digital security, "The Internet of Things", education, and exchanging information on cyber security and cybercrime.[87]

Within the Netherlands, the CSR also helps private companies carry out cyber security "health checks" to identify threats and weaknesses in their cyber security programmes.[88] Furthermore, one of CSR's main contributions to Dutch policy is to identify main trends affecting cyber security. In 2016, for example, they warned against a shortage of cybersecurity professionals, promoting cybersecurity training in general education.[89]

In addition to its numerous publications, the Dutch CSR has also recently worked to create similar cyber security councils in other EU countries.[90] In July 2018, for instance, the UK began to have its own discussions regarding the creation of a Cyber Security Council.[91] Its international efforts focus on the independent advisory role that cyber security councils can play in helping governments to be forward thinking, encourage private participation in helping to shape government policies, and deepen cooperation and open discussions between the public and private sectors.

83 Dutch Cyber Security Council https://www.cybersecurityraad.nl/index-english.aspx
84 Melissa Hathaway and Francesca Spidalieri. (2017) "The Netherlands Cyber Readiness at a Glance." Potomac Institute for Policy Studies, May 2017. http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf
85 Melissa Hathaway and Francesca Spidalieri. (2017) "The Netherlands Cyber Readiness at a Glance." Potomac Institute for Policy Studies, May 2017. http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf
86 Dutch Cyber Security Council https://www.cybersecurityraad.nl/index-english.aspx
87 Cyber Security Council Annual Report 2017 https://www.cybersecurityraad.nl/binaries/CSR_Jaaroverzicht_2017_ENG_def_tcm107-314465.pdf
88 For Example, see Cyber Security Council "Cyber Security Health Check: Medium-Sized Companies" https://www.cybersecurityraad.nl/binaries/NBA_Cyber_Health_Check_ENG_tcm107-356466.pdf
89 Cyber Security Assessment Netherlands 2016 https://english.nctv.nl/binaries/CSAN%202016_def_tcm32-145252.pdf
90 Cyber Security Council Annual Report 2017 https://www.cybersecurityraad.nl/binaries/CSR_Jaaroverzicht_2017_ENG_def_tcm107-314465.pdf
91 "Developing the UK cyber security profession" https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession

Assessment

Academic and practitioners generally agree that cooperation between the public and private sectors and knowledge sharing of cybersecurity incidents will improve the identification and management of the cyber threats. That being said, there remains disagreement over how that knowledge should be shared, and what good knowledge sharing looks like.[92]

In 2011, Luiijf, et. al. compared ten national cyber security strategies, including: Australia, Canada, Czech Republic, France, Germany, Japan, The Netherlands, New Zealand, the United Kingdom, and the United States.[93] Most of the policies acknowledged the important role of cooperation between the public and private sector in cyber security. Beyond that, the authors found significant differences regarding the scope of the strategies, their association with the internet and critical infrastructure, and their relationship with the nation's existing strategic policies.

Unlike other countries that focus solely on cyber security strategies and cyber security centres, the Dutch approach includes an independent advisory entity equally representing the public and the private sector.[94] Arguably, at least part of its success comes from the equal partnership at the table, as well as its independent and high-level nature. While its diverse composition of private and public actors has been praised, Heuvel and Baltink, in their review of Dutch cybersecurity efforts, point out that not everyone feels equally represented,[95] and that often the interests of public and private actors within the Council do not align.[96]

The problem of conflicts of interest between public and private actors has been the focus of a significant portion of the of the literature on PPPs postulating an "incompatibility between private market-based interests and public national security interests".[97] Some authors, however, have suggested that it is possible for the two actors to achieve a common understanding based on a sense of community, that trumps individual strategic interests.[98] This last hypothesis has preliminarily been proved right by Heuvel's and Baltink's findings in the Netherlands. According to the authors, bringing together public and private partners created an "improved understanding of each other's interests and needs, and it has helped better define common goals and criteria".[99]

92 Kristoffer Kjærgaard Christensen & Karen Lund Petersen, (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affair*s, 93(6), 1435-1452.
93 Luiijf, H. A. M., Besseling, K., Spoelstra, M., & De Graaf, P. (2011, September). Ten national cyber security strategies: A comparison. In *International Workshop on Critical Information Infrastructures Security* (pp. 1-17). Springer, Berlin, Heidelberg.
94 The Dutch cybersecurity outfit also include the Dutch National Cyber Security Centrum (NCSC) which is a joint venture between the private sector and government bodies, as well as the National Coordinator for Security and Counterterrorism.
95 Elly Van Den Heuvel and Gerben Klein Baltink (2014). Coordination and cooperation in cyber network defense: the Dutch efforts to prevent and respond. in *Best Practices in Computer Network Defense: Incident Detection and Response*, *35*, 121.
96 Elly Van Den Heuvel and Gerben Klein Baltink (2014). Coordination and cooperation in cyber network defense: the Dutch efforts to prevent and respond. in *Best Practices in Computer Network Defense: Incident Detection and Response*, *35*, 121.
97 Kristoffer Kjærgaard Christensen & Karen Lund Petersen, (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affair*s, 93(6), 1435-1452.
98 Kristoffer Kjærgaard Christensen & Karen Lund Petersen, (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affair*s, 93(6), 1435-1452.
99 Elly Van Den Heuvel and Gerben Klein Baltink (2014). Coordination and cooperation in cyber network defense: the Dutch efforts to prevent and respond. in *Best Practices in Computer Network Defense: Incident Detection and Response*, *35*, 121.

Another critical aspect of the relationship between the public and private sectors on issues of cyber security is the risk of private actors dominating cyber security policy and the subsequent abandonment of responsibility by governments for issues of national and international cyber security.[100] In the Netherlands, however, although the wide majority of critical processes in the area of cybersecurity are in the hands of private parties, [101] there is no indication that the government has withdrawn, giving the private sector free rein.

Representatives of the public sector not only sit in the CSR, but are also actively involved in writing the Cyber Security Assessment Netherlands (CSAN)[102] and responding to threats. The work of the Cyber Security Council was put to the test soon after its establishment, with the DigiNotar cyber incident in which certificates were stolen from a private Dutch registry company.[103] In response, the CSR coordinated between public and private actors, both equally involved in providing an efficient and forward-looking response.[104]

The success of the Dutch Cyber Security Council has resulted in other countries copying the Dutch system and set up their own cyber security councils. For example, in July 2018, the UK launched an initiative to work towards founding their own Cyber Security Council.[105] While by no means perfect, the CSR has created a template for equal partnership at the policy making table to address critical issues related by the cyber security of the Netherlands.

Case study 3 – Infrastructure

Background

Initial cooperation efforts between the public and private sector focused on private sector money funding infrastructure projects.[106] As the great majority of such projects related to critical infrastructure, more structured partnerships, often based on a very solid contractual bases to ensure proper regulation and maintenance, started to develop.[107] Unlike other, less established PPPs, partnerships in infrastructure have a long history. Constituting some of the oldest, and most popular, PPP frameworks, these projects developed in a variety of areas, from prisons to highways, to air and sea ports.[108]

100 Madeline Carr (2016) Public–private partnerships in national cyber-security strategies. *International Affairs* 92: 1. pp 43–62
101 "Resilient critical infrastructure" National Coordinator for Security and Counterterrorism Ministry of Justice and Security. (2018) https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf
102 "Cyber Security Assessment Netherlands CSAN 2018" National Coordinator for Security and Counterterrorism, Ministry of Justice and Security. https://english.nctv.nl/binaries/CSBN2018_EN_web_tcm32-346655.pdf
103 Charles Arthur (2011) "DigiNotar SSL certificate hack amounts to cyberwar, says expert" The Guardian. September 5, 2011. https://www.theguardian.com/technology/2011/sep/05/diginotar-certificate-hack-cyberwar
104 Heuvel, E. V. D., & Baltink, G. K. (2014). Coordination and cooperation in cyber network defense: the Dutch efforts to prevent and respond. in *Best Practices in Computer Network Defense: Incident Detection and Response*, *35*, 121.
105 UK Government "Developing the UK cyber security profession" https://www.gov.uk/government/consultations/developing-the-uk-cyber-security-profession
106 UK Parliament (2011) "Public Accounts Committee – Forty-Fourth Report Lessons from PFI and other projects" https://publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1201/120102.htm
107 The protection of critical infrastructures against terrorist attacks: Compendium of good practices. The United Nations (2018) https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf
108 Darrin Grimsey and Mervyn Lewis. (2007) Public private partnerships: The worldwide revolution in infrastructure provision and project finance. Edward Elgar Publishing.

This third case study looks at public-private partnerships in infrastructure by analysing the case of the Hamburg airport in Germany. Historically, airports around the world were government owned. However, with the privatisation wave of the mid 1980s and1990s, there has been a shift in the ownership and management of airports across the world, specifically in Europe.[109] Not at the forefront of the privatisation wave, the case of the Hamburg airport has nevertheless been considered crucial to test some of the hypothesis of success and failure developed in the extensive literature on PPP in infrastructure.[110]

The main discussions about PPPs in infrastructure security revolve around questions over the nature of the public and private relationship. The Organisation for Economic Co-operation and Development (OECD) has emphasised the importance of coordinating with the private sector, as they are some of the biggest owners of critical infrastructure around the world.[111] To encourage and facilitate this partnership, the OECD had laid out guidelines for the protection of critical infrastructure not only at the state level, but across borders.[112]

The International Airport in Hamburg, Germany: How does it work?

According to the German Federal Ministry of Transport and Digital Infrastructure (BMVI) Infrastructure Plan that was released in 2003, air travel was estimated to double from 1997 to 2015.[113] In order to help cope with the expansions and renovations needed throughout Germany, a number of private partners were brought to the table. This case focuses on the International Airport in Hamburg, which is, today, a shared risk infrastructure public-private partnership.

In Germany, airports and air travel are considered critical infrastructures, defined as "organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."[114] As a result, the aviation administration is governed by the public sector, specifically by the federal states, the federal government, and the German Federal Ministry of Transport and Digital Infrastructure.[115]

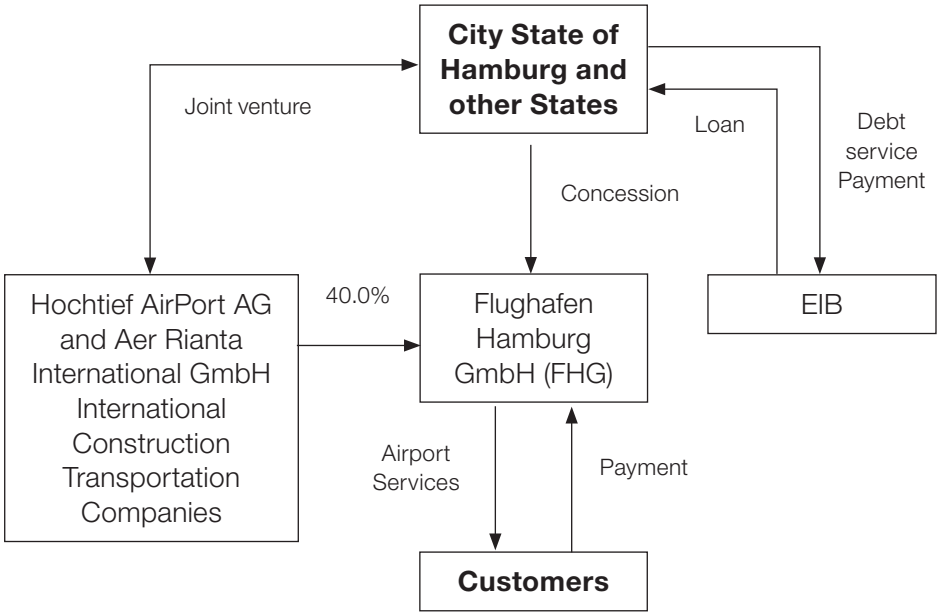
In 1997, a consortium called Flughafen Hamburg GmbH (FHG), made up of the City State of Hamburg (64%), Federal Republic of Germany (26%), and the State of Schleswig-Holstein (10%), sought to dissolve and create a partial privatisation of the Hamburg Airport. In 2000, the German government launched an EU-wide tender, before awarding a 36% share of

109 Tae H. Oum, Nicole Adler, and Chunyan Yu. (2006) "Privatization, corporatization, ownership forms and their effects on the performance of the world's major airports." Journal of air Transport management 12(3): 109-121.
110 Peter Gerber, (2002). Success factors for the privatisation of airports—an airline perspective. Journal of Air Transport Management, 8(1), 29-36.
111 OECD (2013) "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace" https://www.osce.org/atu/103500?download=true
112 OECD (2008) "OECD Recommendation of the Council on the Protection of Critical Information Infrastructure" http://www.oecd.org/sti/40825404.pdf
113 "Federal Transport Infrastructure Plan 2003" (2003) Federal Ministry of Transport and Digital Infrastructure.
114 National Strategy for Critical Infrastructure Protection (CIP Strategy). German Federal Ministry of Interior, Building and Community https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html
115 Federal Ministry of Transport and Digital Infrastructure "Air transport is an important part of the modern transport infrastructure today" https://www.bmvi.de/SharedDocs/EN/Articles/LF/air-transport-modern-infrastructure.html

FHB to a consortium made up of Hochtief AirPort GmbH – now AviAlliance – and Aer Rianta International GmbH.[116] Together, the City State of Hamburg (as majority public partner) and the new consortium (as minority private partner), made up the PPP that is today Flughafen Hamburg GmbH, which runs Hamburg International Airport.[117]

The governing board of the airport includes both public and private parties. All objectives in the PPP have to be agreed upon between the majority public partner, the City State of Hamburg, and the private partner. Furthermore, both public and private partners have veto rights in instances of disagreement. A contract was also written regulating fees for four years, until 2004, when the contract could be renegotiated.[118] In January 2002, the private consortium increased their ownership of the airport by a further 4%, and again in August 2002 to an additional 9%. Today, the private consortium holds 49% and the City State of Hamburg 51% of Hamburg airport.[119]

PPP Structure of International Airport Hamburg AG[120]



116 "History" AviAlliance. https://www.avialliance.com/avia_en/24.jhtml
117 "Case No IV/M.1035 – Hochtief/Aer Rianta/D‚sseldorf Airport: Notification of 20.11.97 pursuant to Article 4 of Council Regulation N/ 4064/89.
" Commission of the European Communities.
Notification of 20.11.97 pursuant to Article 4 of Council Regulation N/ 4064/89
118 European Commission (2004) "Resource Book on PPP Case Studies". https://ec.europa.eu/regional_policy/sources/docgener/guides/ppresourcebook.pdf
119 "History" AviAlliance. https://www.avialliance.com/avia_en/24.jhtml
120 European Commission (2004) "Resource Book on PPP Case Studies". https://ec.europa.eu/regional_policy/sources/docgener/guides/ppresourcebook.pdf

How is International Airport in Hamburg Unique?

PPPs in infrastructure are much more contractual than other public-private partnerships, as the main goal of an infrastructure PPP is the financing, management, design, construction and maintenance of infrastructure.[121]

The International Airport in Hamburg constitutes a partial privatisation public-private partnership, where the public partner, the City State of Hamburg, maintains majority control of the relationship. It operates on a "future contract model" and with a "price cap review board". The future contract model consists of the airlines and the airport agreeing on a pre-contract, the contents of which are authorised by the public authorities and then included in the contract under public law. The board, instead – which must be consulted regarding all fee changes – guarantees that both public and private partners from the airport and airlines have a voice.

Assessment

The European Court of Auditors found that PPPs in infrastructure were "more likely to achieve efficiency gains than traditional projects". However, it also argued that often the benefits that a PPP could offer did not come to fruition, due to timing and cost issues.[122] This has been the case, at least to a certain extent, with the Hamburg airport. The European commission argued, since the public sector had to maintain majority ownership of the airport in compliance with German laws the speed of the development of the airport has been slowed down.[123] From the financial point of view, the decision by the German Federal Government and the State of Schleswig-Holstein, who alongside the City State of Hamburg were original owners of the airport, to withdraw from the project once converted into a public-private partnership meant a significant loss of financial partners. In reality, this did not have a significantly negative impact in this case,[124] probably also thanks to the €220 million loan granted by the European Investment Bank,[125] as well as the fact the private consortium has been able to increase its share in the airport from the original 36% to its current 49% hold.[126]

Research looking at profit margins and efficiency of airports – mainly in Europe – suggests that those owned by a private majority are significantly more successful than airports under other forms of ownership agreements. [127] The Hamburg airport case seems to contradict these findings, or at least represent an exception to the rule. Despite 60% of shares in the hands of the public sector, the PPP model adopted in this case has proved successful, with air traffic in the first year of the public-private partnership

121 H.W. Alfen, (2010). Public Private Partnership (PPP) as part of Infrastructure Management solutions–a structural approach of delimiting PPP from other Private Sector participation Models. In TG72-Special Track 18th CIB World Building Congress May 2010 Salford, United Kingdom (p. 13).
122 European Court of Auditors (2018) "Public Private Partnerships in the EU: Widespread shortcomings and limited benefits" https://www.eca.europa.eu/Lists/ECADocuments/SR18_09/SR_PPP_EN.pdf
123 European Commission (2004) "Resource Book on PPP Case Studies". https://ec.europa.eu/regional_policy/sources/docgener/guides/pppresourcebook.pdf
124 European Commission (2004) "Resource Book on PPP Case Studies". https://ec.europa.eu/regional_policy/sources/docgener/guides/pppresourcebook.pdf
125 European Commission (2004) "Resource Book on PPP Case Studies". https://ec.europa.eu/regional_policy/sources/docgener/guides/pppresourcebook.pdf
126 "History" AviAlliance. https://www.avialliance.com/avia_en/24.jhtml
127 Tae H. Oum, Nicole Adler, and Chunyan Yu. (2006) "Privatization, corporatization, ownership forms and their effects on the performance of the world's major airports." Journal of air Transport management 12(3): 109-121.

surpassing predictions.[128] Gerber (2002), in his article on the 'success factors for the privatisation of airports', went as far as to describe the airport's "future contract" system an "ideal solution", and the "fee cap review board" a successful "system partnership for growth"[129]. The board is in fact especially important because it gives a voice to the airlines, which strictly speaking are not part of the PPP that runs the airport. As Gerber (2002) notes: "In this manner, a balance of power between all the stakeholders is achieved.[130]

Also, the European Commission recognises the price-cap regulation system among one of the specific strengths of the Hamburg Airport PPP symbolising willingness of the all the parties to compromise. Another aspect which seems to be key in explaining the success of the Hamburg airport PPP and which has been pointed out by the Commission is the importance of public and private partners agreeing on most present and future terms before the finalisation of the sale.[131] This allows for clear rules and transparent contractual instruments in case of disagreements that are essential for a successful management of the relationship. Last but not least, the fact that both the public and the private actors within the government board have a veto right, has further strengthened the equal relationship between the private and the public sector.

In a nutshell, the Hamburg airport PPP seems to meet all the conditions allowing for a successful collaboration between public and private actors, therefore creating a "positive impact for users, operators and current as well as future taxpayers".[132] In fact, after the implementation of the Hamburg Airport PPP, the German government launched the Federal PPP Task Force to monitor and enforce future public-private partnerships in Germany.

128 Peter Gerber, (2002). Success factors for the privatisation of airports—an airline perspective. Journal of Air Transport Management, 8(1), 29-36.
129 Peter Gerber, (2002). Success factors for the privatisation of airports—an airline perspective. Journal of Air Transport Management, 8(1), 29-36.
130 Peter Gerber, (2002). Success factors for the privatisation of airports—an airline perspective. Journal of Air Transport Management, 8(1), 29-36.
131 European Commission (2004) "Resource Book on PPP Case Studies". https://ec.europa.eu/regional_policy/sources/docgener/guides/pppresourcebook.pdf
132 Antonio Estache and Tomás Serebrisky. (2004) "Where do we stand on transport infrastructure deregulation and public-private partnership?". The World Bank.

6 Conclusion

As this report has shown, public-private partnership are an interesting and developing area of public policy. While there remains no agreed definition of PPP, the subject is increasingly shaped and defined by its practice. This includes many of the “experiments” and experiences with PPPs in the area of security.

As our case studies have demonstrated, collaborations need to be sector-specific and cannot be generalised. Yet, it is vital for both sides to have clear expectations and set specific goals for the PPP to be considered successful. As well as the contractual elements of the relationships, benefits derived from the development of personal relationships and regular interactions, which enabled actors on both sides to better understand each other and anticipate actions.

Overall, we believe there is great potential for public-private partnerships in all areas of public security. As our case studies have shown, these come in many shapes and sizes, and need to more systematically evaluated and studied by researchers. But there can be no doubt that private sector actors are interested and willing to be “enlisted” in making our societies more secure – for their own benefit, and that of society as a whole.

Crime Terror
Nexus

THE CRIME TERROR NEXUS

The Crime Terror Nexus is a project that investigates links between crime and terrorism, and identifies better ways to counter them.

Over the course of 18 months, we are documenting links between crime and terrorism across the European Union. Our findings are disseminated through reports, events, and workshops.

We are partnering with officials and local stakeholders to create new and innovative approaches that contribute to countering crime and making our countries safer.

The Crime Terror Nexus is a project of Panta Rhei Research Ltd. It is funded by PMI IMPACT, a global grant initiative of Philip Morris International that supports projects against illegal trade.

Panta Rhei Research Ltd. is fully independent in implementing the project and has editorial responsibility for all views and opinions expressed herein.

For more information, visit **www.crimeterrornexus.com**.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact Katie Rothman: katie@crimeterrornexus.com

Registered address: Panta Rhei Research Ltd.,
37a Great Percy Street, London WC1X 9RD, United Kingdom

www.crimeterrornexus.com