

HOT SPOTS OF SECURITY HIGH TECH
Mapping Emerging Trends in the
International Market of Promotion of
Security Technologies

James Alexander
Emmanuel-Pierre Guittet

HOT SPOTS OF SECURITY HIGH TECH

Mapping Emerging Trends in the International Market of Promotion of Security Technologies

James Alexander
University of Manchester

Emmanuel-Pierre Guittet
University of Manchester

Nesta Working Paper 15/01
January 2015

www.nesta.org.uk/wp15-01

Abstract

There is a voluminous and significant body of academic literature on security, encompassing a range of emphases and points of departure. Much of this body of work is mainly concerned with the size, sectorial composition and growth of the commercial security industry and the multitude of security products offered. And, indeed with a global market for security and service estimated at £45 billion a year with a predictable further stellar growth, there is some grounded reason to study the key features of such a global market. This paper is a contribution to that academic literature dedicated to the analysis of the local and global markets of security. Its specific focus though is upon a neglected part of that literature: the international security trade fairs and exhibitions. The aim of the paper is twofold: first, to assemble and coordinate research materials in order to track the historical and spatial evolution of these international security trade fairs and exhibitions and secondly, to show how these places are pivotal in the dissemination of not only tools and high tech security technologies but also in the propagation of a particular mind-set of the consumption of security commodities.

Keywords: Technology policy, Security Science, Digital Social Science.

Corresponding author: Emmanuel-Pierre Guittet, 4.010 Arthur Lewis Building, University of Manchester, Oxford Road, M13 9PL, Emmanuel-pierre.guittet@manchester.ac.uk.

The Nesta Working Paper Series is intended to make available early results of research undertaken or supported by Nesta and its partners in order to elicit comments and suggestions for revisions and to encourage discussion and further debate prior to publication (ISSN 2050-9820). © Year 2015 by the author(s). Short sections of text, tables and figures may be reproduced without explicit permission provided that full credit is given to the source. The views expressed in this working paper are those of the author(s) and do not necessarily represent those of Nesta.

TABLE OF CONTENTS

Activity information	2
Table of figures	2
Executive Summary	3
1. Scope of the report and methodology used	4
2. Review of the Literature	5
Introduction.....	6
Security and risk management	6
clustering and knowledge exchange.....	8
3. Historical and geographical developments of the market of security	11
Introduction.....	12
Definitions and Dataset	12
historical configurations	13
Spatialisation and joint-ventures.....	14
4. Mapping the online world of the security market	17
Introduction.....	17
Extent of the digital network	18
Contents of the digital network.....	19
Spaces of promotion and the transfer of knowhow.....	21
5. Conclusions	26
References	27

ACTIVITY INFORMATION

ACTIVITY TITLE	Hot Spots of Security High Tech. <i>Mapping Emerging Trends in the international Market of promotion of Security Technologies</i>
ACRONYM	HOSSET
PERIOD	March – July 2014
AUTHORS	James J. Alexander and Dr. Emmanuel-Pierre Guittet, University of Manchester – School of Social Sciences - Politics

TABLE OF FIGURES

Figure 1 - Cumulative Total Events Post-1990..... 14

Figure 2 - Types of Organisers 15

Figure 3 – Non-Contiguous Cartogram of Geographic Distribution of Trade Fairs..... 15

Figure 4 – Exhibitions grouped by exhibitor number 16

Figure 5 - Exhibitions grouped by visitor number..... 16

Figure 6 – Close-up of Most Connected Points 20

Figure 7 - Wordcloud of Most Connected Points 20

Figure 8 - IssueCrawler Network of Key Sites of Interaction 22

Figure 9 - Geographic Map of IssueCrawler Network..... 23

Figure 10 - Issues Discussed..... 24

Figure 11 - Wordcloud of sites most discussing 'CCTV' 25

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of Nesta.

EXECUTIVE SUMMARY

There is a voluminous and significant body of academic literature on security, encompassing a range of emphases and points of departure. Much of this body of work is concerned with the size, sectorial composition and growth of the commercial security industry and the multitude of security products offered. And, indeed with a **global market for security and service estimated at £45 billion a year** with a predictable further stellar growth, there is some grounded reason to study the key features of such a global market. The project HOSSET is a contribution to that academic literature dedicated to the **analysis of the local and global markets of security**. Its specific focus though is upon a neglected part of that literature: the international security trade fairs and exhibitions. The aim of the project HOSSET was twofold: first, to assemble and coordinate research materials in order to track the historical and spatial evolution of these international security trade fairs and exhibitions and secondly, to show how these places are pivotal in the **dissemination** of not only **tools and high tech security technologies** but also in the propagation of a particular mind-set in the **consumption of security commodities**.

The present report thus maps the historical and spatial evolution of the international exhibitions and trade fairs and an analysis of their online presence and their use of social media. It finally provides a set of reasoned conclusions about the evolution of the international market of promotion of security technologies and suggests future research trajectories. This report is divided into five sections. Section 1 recaps the scope of the project and the methodology used. Section 2 is a short review of the literature and offers a theoretical underpinning to the project. Section 3 is dedicated to the historical and spatial evolution of these international security trade fairs and exhibitions. Section 4 exposes the digital lives of these international security trade shows and fairs. Section 5 provides some conclusions and potential future research trajectories. The report concludes:

- There has been negligible examination and theorization of the evolution and importance of **international security trade fairs and exhibitions** in the dissemination of specific **imagined scenarios of risk and security**.
- In addressing these empirical and theoretical lacunae, the present project HOSSET draws upon **primary research** into the **historical and geographical evolutions** of these international security trade fairs and exhibitions.
- The present report provides an **original and empirically grounded examination** of the evolution of both the physical and online presence of every international security technology trade fair and

exhibition, and deploys the latest **digital media analysis** to analyse these flows of information and quantify this knowledge exchange and dissemination.

- It argues that these international security trade fairs and shows are **hot spots of security** and that the growth in size and number of these places are made sense of within a context of **changing sensibilities towards security** as much as they are part of the process.
- It also suggests that this research cannot be entirely definitive and should be complemented with a more in depth analysis of the **core governmental and societal** shifts that have catalysed these dynamic processes.

1. SCOPE OF THE REPORT AND METHODOLOGY USED

Since the 1980s, the number of international trade shows dedicated to the promotion of high tech security devices has grown exponentially. As of 2013, there were more than 160 international exhibitions specialized in a myriad of security technologies and defence tools - surveillance, protection, police, weapons and more – in all corners of the globe. Last year alone, 565 days were spent displaying such tools, exhibited at 55,441 stalls and seen by 388 9350 people. The technology displayed at these events continues to develop at a rapid pace. Whether it is by ‘hactivist’ groups or security service surveillance, new innovations are developed and deployed at a speed that outstrips legislation (Cornish 2010). Thus, it is of no surprise that emerging trends and important developments in the field of security technologies are of increasing interest to governments and private actors alike. However, the relationship between new technologies, their justification and promotion, and the spaces in which they are marketed is by no means simple. Previous research we have conducted at trade fairs since 2006 suggests that they are far more than simply places of economic exchange. **They facilitate, and are highly concentrated but short duration sites, or “temporary hot spots”, for the exchange of knowledge and best practice of how to say and to do security.**

The advent of social media has only magnified this effect. With Twitter and Facebook giving trade shows a year-round audience of business, government, and private customers, **their role as hot-spots for knowledge exchange is becoming increasingly permanent.** This can be easily seen through their online presence consisting of much more than advertising the next event – they blog and comment on new developments in both technology and security policy more broadly, disseminating their opinion much more widely than the event itself could hope to achieve. Thus, the goal of this research has been to deploy the latest in digital media analysis to analyse these flows of information

and quantify this knowledge exchange, in order to highlight characteristics of emerging leaders in the future of promoting security technologies. To conduct this study, we have developed a specific approach and related research tools. Until recently, generating meaningful quantitative data from complex online networks has been a challenging task. However, we have been able to utilise and develop the open-source **Medialab and Digital Methods Initiative Tools**, in collaboration with their creators, in order to fill this void. The individual tools used will be described in detail in Section 4 of this report, however the overall purpose of their deployment has been in order to trace not just the direction and size of information exchange between actors, but to quantify the content of this information and to trace its dissemination, and importantly impact, through the wider network. Thus, such tools enable an analysis of which sites are likely future hot spots, and what characteristics they exhibit.

2. REVIEW OF THE LITERATURE

KEY FINDINGS

- Since the 1990's **security policy** has been reoriented away from calculable 'traditional' military threats towards varied and potentially **unknown risks**. The terrorist attacks of September 11th are a primary example.
- In order to calculate, **predict and profile** these risks, increasingly **complex security technologies** have been called upon, the bulk of which have been developed by the private sector.
- Little attention has been paid to the trade fairs and exhibitions (B2B and public) where these tools are marketed, however it is in these **clusters** where one can witness the marketing and sale of the 'latest and greatest' tech fixes from an ever increasing range of private sector actors.
- Research into these clusters has shown that they are about more than simply economic exchange, but are sites of 'buzz' – **knowledge exchange and transfer** – that builds a shared language and outlook.
- The online and physical elements of modern **trade fairs represent a hybrid or super-cluster**, absorbing the benefits of both temporary and permanent spaces without the disadvantages of either.

INTRODUCTION

This section draws primarily on two groupings of literature – that concerned with *security* (International Relations, Security Studies, Criminology and Sociology), and that concerned with *hot spots* of knowledge exchange in business (Human Geography and Economics).

SECURITY AND RISK MANAGEMENT

Some of the most prevalent of modern day technologies are those deployed in the name of 'security'. From the banal and ubiquitous CCTV cameras on our streets or in our public transport to massive databases deployed at the transnational level in order to sort traveller details and profile potential risks, technological fixes for security issues are everywhere, progressively more interconnected and in ever increasing numbers. However, a more nuanced discussion of such technologies extends well beyond the materiality of the tool itself. The genesis of these technologies begins long before they are deployed and integrated into everyday life. Their evolution is messy and complex, their meaning and function inseparable from the practices that are associated with them. Thus, if we wish to ask questions about the evolution of such tools in the marketplace, as well as likely trends in the security business sector, it is an investigation of the development, diffusion and normalisation of these practices that allows us to fully appreciate the *process* of technology, and more importantly what this means for the practice of *security*.

Important steps have been taken to engage with the idea that contemporary threats have become uncertain, unlimited and imminent to the spaces of everyday life (e.g. Rasmussen 2006, Amoore 2007, Amoore and De Goede 2008) to assess the ways in which conceptions of risk "tear at the social fabric" (Ericson 2006) and affect the security agenda. Thus, as David Garland notes, " 'late modernity' is lived...in a mode that is more than ever defined by institutions of policing, penalty, and prevention" out of a desire for "the management of risk and the taming of chance" (Garland 2001, 194). What is called for is an analysis of how these imaginaries of low-probability but high-impact threats are incorporated, negotiated and reoriented through a multitude of practices that sediment and concretise the dominant security narrative of the day. These risks have, as a growing body of literature claims, resulted in a modern day security apparatus that addresses itself to threats that are irregular, incalculable, and in important ways unpredictable (Amoore and de Goede 2008, Aradau and van Munster 2007; 2011; Massumi 2009). These authors point out that an understanding of contemporary threats as dispersed and uncontrollable phenomena has fostered a

mode of security that aims to identify threats at an early stage, and to intervene accordingly. The central claim here is the notion that our **current understanding of security diverges from traditional means of risk management** based on causal and calculative knowledge in that it functions on the very limits of knowledge. Here, security intervention involves a more imaginative orientation toward the future and ‘anticipatory work’ that includes storytelling, scenario planning, and the performance of exercises (Anderson 2010; Aradau and Van Munster, 2011).

This leads the security agenda to move away from intelligence-led projects (based on traditional methods of information gathering and analysis) and towards imagination-led projects, which are necessarily less ‘scientific’ and speculative in nature. This attempt at risk management calls for the construction of convincing storytellings of anticipated worst-case scenario futures that must be protected against. Thus, the traditional barriers to entry for firms wishing to enter the lucrative security technology market are reduced for two reasons. Firstly, as they do not need the same access to classified and covertly-obtained information that made intelligence-led operations the preserve of the police and security services. Secondly, because the private sector is already adept at constructing convincing imaginaries in which their products are required through years of advertising experience. In a similar vein to the “commodification of security” (Loader and Walker, 2007; Bigo et al. 2014), **imagination becomes a valuable commodity in its own right and when the focus is on an unpredictable future, can be touted as knowledge**. This process opens up the security narrative to the technology firms themselves and gives them a chance to make their imagined future the dominant one on which risk and security decisions are made. Indeed, it is perpetuating and reproducing this discourse of inescapable and perpetual risk and threat that is of primary concern as it is precisely this narrative that lends continued legitimacy to the producers of security tools as the only potential solution – sustaining them in the marketplace.

The claim is that such anticipatory, speculative, planning is more often than not based on data-led technologies and the notion that threat patterns can be recognized at an early stage through the creative combination and mediation of a vast array of seemingly heterogeneous data points, using “visionary techniques” that have been likened to “alchemy” (Amoore and de Goede 2008, Amoore 2011). Thus to excel at risk management, one needs not only the best imagination but the best storytelling ability – the ability to make one narrative on risk the dominant one. Building on this is the idea that legitimising security concerns is achieved through “the discursive ability to produce an image of the enemy with which the audience identifies” (c.a.s.e. collective, 2006: 457). Therefore a key claim of critical security studies literature is that this notion of *imagination* is fundamental to this

situation when the concept of risk is incorporated – if you can capture the imagination of both the public and policymakers alike, you have the ability to define a future in which your own solutions are the only possible response. Indeed, this logic of security has an important impact on security technologies and their manufacturers. **As the net of potential risk is cast wider in the search for ever-more tech savvy terrorists and others considered a risk, so the list of technology used to hunt them widens also.** As new firms are encompassed within the security arena (such as those traditionally considered in the information communications technology industry), the knowledge base required to operate all these systems spreads out accordingly. This can be seen as a levelling of the security industry playing field, giving the private sector ever greater means to challenge the dominance of the security services and put forward their own imagined futures of risk and threat.

CLUSTERING AND KNOWLEDGE EXCHANGE

Having established the need to study the market for security technologies if we wish to understand developing trends in security more generally, this project then contends that **whilst the economic transactions within trade fairs, conventions and exhibitions are certainly part of their logic, they are not the primary component.** Rather, these spaces facilitate a wide-ranging and rapid exchange of information and technical know-how. They can be thought of as ‘temporary clusters’; hotspots of intensive exchange of knowledge, new ideas and network building. There is a large body of literature concerned with research into *spatial clustering* amongst firms – essentially industry agglomeration (e.g. Sabel 1989; Porter 1994; 1998; Scott 1998, Malmberg 1996; Maskell 1998 to name but a few key examples). Whilst this literature is primarily concerned with assessing the impact of *geographic* clustering of firms and the effects that has, it has direct implications for how we can understand the processes of online knowledge exchange and interaction exhibited by the marketplace. Indeed, in facilitating these interactions both online and at the physical events, trade fairs and exhibitions can in fact become thought of as **hybrid hotspots** that encompass the benefits of the highly concentrated temporary cluster as well as the knowledge processing abilities of more permanent structures. Thus, they enable **knowledge pipelines to be constructed across the industry that encourages cooperation, information sharing, common language and the development of best practice.**

Yet what is the value of this kind of clustering? It has been claimed that “the localized cluster is *the* territorial configuration most likely to enhance learning processes [within firms]” (Malmberg and Maskell 2002, 428). Indeed, many of the most successful individual businesses, and sectors, operate within such clusters. From Cambridge to the Slovakian Aerospace cluster it seems being close to related competitors has something to offer when it comes to building a successful business.

Traditional analysis of these clusters (ie Marshall 1920; Krugman 1991) suggests that essentially the benefits of being spatially linked are threefold: they can share the costs of collective resources amongst themselves, including local infrastructure; they develop a localised specialist labour force that increases skill level; and that costs are reduced as transactions between local firms, including shipments, are negligible, without having the inflexibility of full-scale integration. Such an analysis provides little of use to the case of the clustering we see in the digital realm – the infrastructure is already provided by the social media platforms, the workforce is no more localised than it was previously, and transaction costs are not reduced any more than they would be by more conventional electronic communication like email. However, more recent research has raised the prospect of *knowledge spillovers* as a result of spatial clustering (see also Nesta 2013).

Here we introduce the idea of a local *milieu*, a social environment of firms, in which various forms of spillover can be stimulated – learning, innovation and so forth. This idea of knowledge exchange and spillover has received a great deal of study (ie Porter 1990; Malmberg et al. 1996; Maskell et al. 1998; Malmberg and Maskell 2002), from which is derived the essential idea that not only are learning and innovation stimulated by such clustering, but so too is dynamism and flexibility in the face of the broader market. In essence, “a local culture with specific norms, values, and institutions (formal and informal) makes it possible to transfer tacit forms of knowledge from one actor to another” (Malmberg and Maskell 2002, 433). In short, the way the culture of the local milieu develops drives a climate in which firms continue to innovate and learn. Perhaps one of the most important parts of this process is the way spatial clustering has been observed to build relationships and trust between firms – keeping to more agreements, sharing tacit information between employees and making sure negotiations tread similar paths (Maskell 2000).

Whilst much of the clustering literature treats the phenomenon as permanent and durable, there is some work that focusses on the temporary sites of clustering – the very trade fairs and exhibitions that are under study in this report. These all address the question of whether, as **trade fairs and exhibitions are temporary sites by nature, they can exhibit the same function as clusters of**

knowledge exchange and spillover (Maskell et al., 2004; Maskell et al., 2006; Barthelt and Shuldts 2008; 2010; 2011; Rubalcaba-Bermejo and Cuadrado-Roura, 1995).

There is a consensus amongst these studies that these temporary sites do indeed exhibit similar characteristics to the more permanent groupings we have discussed above, just in a more periodic form. Trade fairs and exhibitions can certainly be used in much the same way as other clusters to acquire information about competitors, suppliers and customers and their technological choices – simply attending the event itself is enough to observe and compare with the competition. The event itself can certainly provide a rich arena for learning processes (Maskell et al. 2004). The coming together of employees and firms specialised in similar areas are able to come together and meet during trade fairs and exhibitions, providing the ideal space for learning and problem solving to develop. Trade fairs also bring competing firms together which would normally not interact, either through simply being too far apart or through not knowing each other exist. Trade fairs provide multiple chances for firms to observe and compare their products and wider business strategy with the competition. It is simple enough to look at the exhibits of rivals, innovations or indeed entirely new fields of business. In the same vein, the way customers react to each firms stand at an exhibition can also be observed and gauged in order to place oneself in the market.

It is exactly this trust and community building that is key to both temporary and permanent clusters. Importantly, activity that could be construed as *corporate transactions*, despite the measurable effectiveness of clusters, is rarely seen in practice inside the clusters themselves (Barthelt 2004; Maskell et al. 2004) and thus there is much more going on than simply being able to measure the economic input and output of clusters (Maskell and Malmberg 2002). We can see this as a process of building “global knowledge pipelines” (Maskell et al. 2006) – the establishment of trans-local links in order to obtain new technologies and ways of thinking. Working differently, but related to the idea of a *buzz*, these pipelines are purposeful and sought out attempts to build trans-local relationships that can result in new kinds of knowledge transfer and recombination, thus ensuring the long term stability of the cluster itself – in short ensuring that they can benefit from outside knowledge. Combined and intertwined with the buzz at a local level, this information about new markets and technologies can be filtered, understood, and re-appropriated in order to take maximum advantage.

Thus the temporary cluster and the permanent cluster exhibit many of the same properties, and complement one another. They are both sites for generating knowledge spill over, community and a shared sense of purpose, language and innovation thanks to their easily accessible buzz. The

temporary cluster is also the perfect site for forging global knowledge pipelines – connecting new firms, new knowledge and new technology to the local scene and incorporating the best of what it has to offer. This is helped by the fact that the temporary cluster is itself a *hot spot*. It is compressed in both space and time to create an intense, short burst of interaction and knowledge exchange. The permanent cluster, on the other hand, has the established infrastructure to filter and sift this intense burst of data into its most useful components. In short, the “value of knowledge gained in temporary clusters will multiply when inserted into the buzz of a permanent cluster” (Maskell et al. 2004, 22).

The value of **social media and other digital interactions** is that it has taken **things outside of the trade show walls and makes the events a year round**, if digital, phenomenon. The starting point of analysis for this project is that these spaces in fact represent a new form of *hybrid* clustering that contains characteristics of both types of cluster. The epicentre, the site of intense knowledge spill over and pipeline building that is the event itself represents a hot spot of the exchange of knowledge and best practice, with all the attendant benefits we have discussed. **But in removing the need for a geographic co-locality for the permanent cluster by replacing the spatial closeness with a digital version, trade shows and exhibitions can see something of a ‘heat-soak’ from this temporary hot spot out to a wider, more solid and long lasting, cluster. If the two types of clustering complement one another and the firms that participate in them, then the hybrid clustering of new trade show environments creates something of a super-cluster, absorbing the benefits of both without the disadvantages of either.** Indeed, creating a more permanent extremity to the hot spot itself can only increase the speed with which firms are able to build, and then maintain, relationships as these can be fostered in between the actual events themselves, making their yearly meetings even more productive and intense, occurrences.

3. HISTORICAL AND GEOGRAPHICAL DEVELOPMENTS OF THE MARKET OF SECURITY

KEY FINDINGS

- Although security technology trade fairs have enjoyed a long history, **since 1990 they have grown rapidly** at a pace of more than 20 new events per year.
- The dataset for this report consists of **164 international B2B and public trade fairs** and trade show dedicated to security and defence tools.
- Whilst there has been a worldwide increase in the number of trade fairs, with a resultant spread in their distribution, there is still a **concentration of events with a European base**.
- The organisers of these events are varied, however **75% are private** (both national and international) entities.

INTRODUCTION

This Section 3 covers a brief analysis of the key elements of the dataset¹. It intends to provide an overview to provide a physical context to the digital analysis that follows in Section 4. We begin by briefly outlining our collections methods, before charting the historical and geographical evolution of the markets of promotion for security technologies.

DEFINITIONS AND DATASET

For the purpose of the present report, we use a common and generally accepted definition of trade fairs and exhibitions. The following is generally and widely admitted - **trade fairs and exhibitions are market events of a specific duration, held at intervals, at which a large number of companies present the main product range of one or more industry sectors**, with trade fairs selling on the basis of samples and exhibitions providing information for the purposes of sales promotion. Trade Fairs predominantly attract trade and business visitors (B2B), whereas exhibitions predominantly attract the general public.

Additionally, for the purposes of examining the knowledge exchange within the marketplace (and indeed the limited scope of a project such as this), **only trade fairs and exhibitions of an international nature are considered**, meaning at least one exhibitor in attendance comes from outside the host nation.

The database itself has been built from a number of sources. Primary amongst these are the fair/exhibition database websites. These sites make their living from providing listings for upcoming events across the entire exhibition spectrum, advertising related events, selling exhibition space and driving visitor registrations. Two of the largest portals of this type are www.expodatabase.com and www.biztradeshows.com. These provide the ideal starting point for data collection as their websites are specifically designed to be navigated by sector and directing visitors to related events. Furthermore, their continued existence and revenue is predicated on accurate and regularly updated listings, thus their listings are almost comprehensive. They often provide all of the required information, from location to visitor numbers, and this information has been corroborated by referring to multiple databases as well as the main site for the exhibition itself. Furthermore, we

¹ Please see the 'Documents' section of MappingSecurity.net for the full dataset. All data is based on 2013 entries as the latest events assessed and documented.

have also drawn on information provided by the Union des Foires Internationales (UFI), known as the global association of the exhibition industry to complement the other sources.

In the database we have collected information on:

- Name/Acronym
- Date of inception
- Host country
- Host city
- Target Audience
- Regularity of event
- Business sectors covered
- Size (in terms of number of exhibitors)
- Size (in terms of visitors)
- Length of the event
- Parent company
- Website address

Thus the database on which this project is based represents a **solid picture of the international spaces of promotion for security technologies that are currently operated worldwide as of 2014.**

HISTORICAL CONFIGURATIONS

Since the beginning of the 1990's, trade shows and exhibitions devoted to security, surveillance and defence have known a development never encountered before. In 1990, there were less than 40 such events worldwide. **Whilst there has been massive growth since then, this phenomenon is not new.** Indeed, exhibitions such as Le Bourget and the Berlin Air Show (both dedicated to aeronautics, space, and defence related tools) started as early as 1909. The first international exhibitions to open outside Europe are Asian Securitex in Hong-Kong (1990), Safety & Security Asia in Singapore (1991), GITEX Dubai (for Gulf Information Technologies Exhibition) in 1992 and IDEX in Abu Dhabi in 1993. It is not before the mid-1990s that security trade shows and trade fairs opened in Eastern Europe. Russia first opened the doors to new security exhibitions with INTERPOLITEX in 1992. Further afield, the first Chinese and Vietnamese security trade fairs opened to international audiences during the same decade (Security China in 1994 and Vietnam Telecom in 1996). **Since 1990, there have been an average of 20 new events launched every 1-2 years**, culminating with CLOUD CONNECT (China), dedicated mainly to ICT; Forensics Europe Expo (United Kingdom), dealing with biometrics, CCTV and covert surveillance systems and SICUR LATINOAMÉRICA (Chile), dealing with disaster control, emergency management and safety equipment. All of these events (and more) debuted in 2012/3.

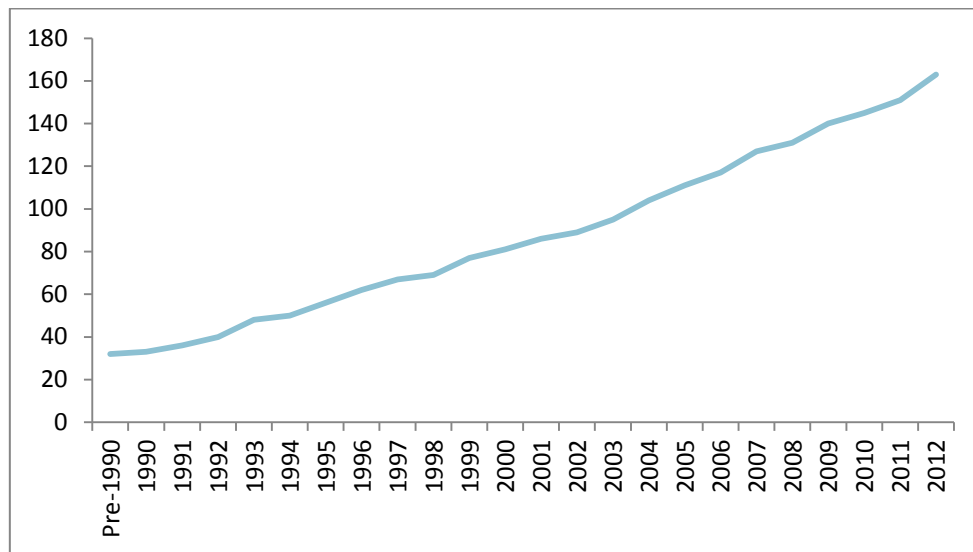


Figure 1 – Growth in Number of Events Post-1990

This historical data demonstrates not only the explosion in supply and demand for security tools and technologies broadly, but also the degree to which **the marketplace has diversified away from ‘traditional’ defence products towards a more comprehensive catalogue** that covers counter-insurgency to ICT and cybersecurity. It is also important to note that this broadening has also been accompanied by an increasingly accessibility to events which once were confidential, even secretive, in their operation. Indeed, exhibitions are increasingly accompanied by conferences, workshops and open key-note addresses from key figures in industry and government (O’Reilly 2010).

SPATIALISATION AND JOINT-VENTURES

Prior to 1990 these events were over 60% European, staged in Western European countries and promoting primarily European products. As of 2013, this figure stands at only 40% with a much wider global spread. Pre-1990 the organisers of these events were mainly governmental bodies (such as the SOFREMI in France or the Defence and Security Organisation – DSO – in UK) and trade associations (like the British Security Industry Association, BSIA). More recently, there has been a rise in some not-for-profit federations or associations organizing their own fairs in a joint venture with private companies. In some instances, fairground owners are also the exhibition organizers. A number of European fair companies have started joint ventures with foreign fair organizations located in regions like the Middle East or the Asia/Pacific, or indeed have setup their own operations there, capitalising on the brand value of the exhibition itself (IFSEC being a prime example, launching

shows in South Africa in 2012, India in 2007 and Turkey in 2013 to capitalise on their already strong UK-based identity).

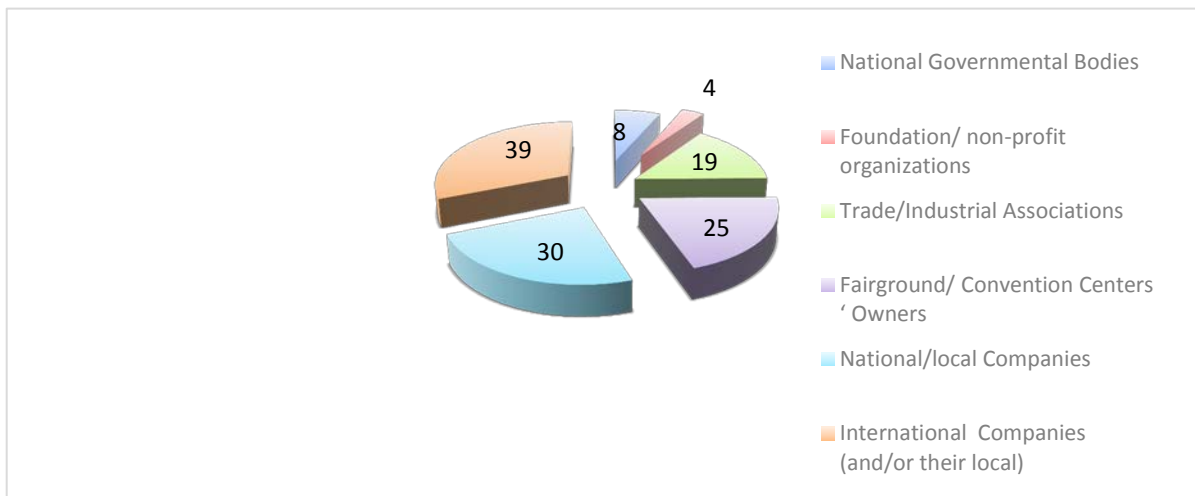


Figure 2 - Types of Organisers (%)

Whilst there has been a worldwide increase in the number of trade fairs and exhibitions, with a resultant spread in their distribution, there is still a concentration of events with a European base. This concentration is even more marked if we assess the parent organising bodies of such trade fairs, where we find that over 66% remain European-based, as demonstrated by Figure 3, below.

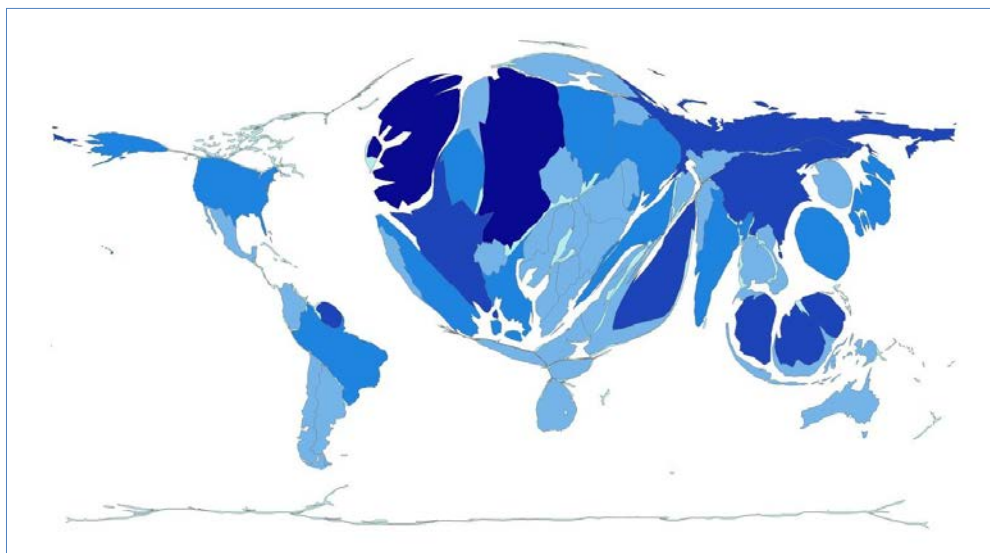


Figure 3 – Non-Contiguous Cartogram of Geographic Distribution of Trade Fairs

In terms of scale, the smallest event with regards to exhibitors involved just 10 stands (ALARME KILECE in Poland) and the biggest involved over 2000 (Paris Le Bourget, France). 68% of the trade

shows and exhibitions covered in the database involve between 10 and 300 exhibitors (companies, associations and governmental bodies alike).

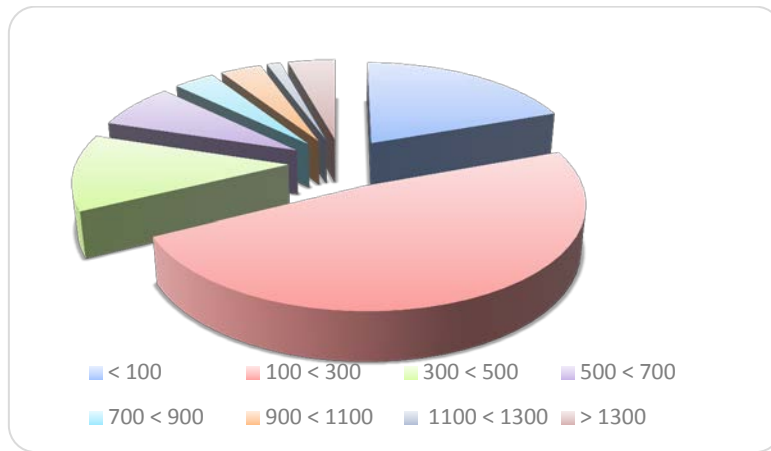


Figure 4 – Exhibitions grouped by exhibitor number

In terms of visitors, the smallest event considered had just 400 visitors (OMNICARD EXPO - The world of smart ID solutions) and the biggest 315,000 visitors (Paris Le Bourget, France). 50% of the exhibitions considered here are attract between 400 and 10,000 visitors (public and B2B alike) with 35% of them attracting between 10,000 and 40,000.

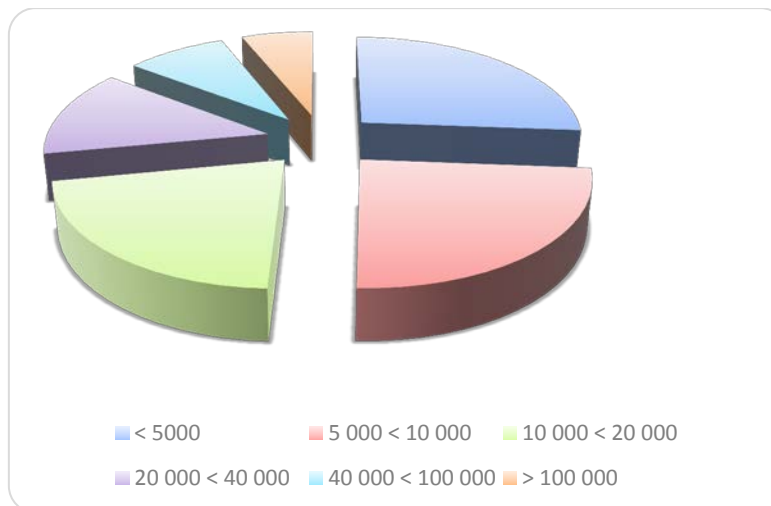


Figure 5 - Exhibitions grouped by visitor number

4. MAPPING THE ONLINE WORLD OF THE SECURITY MARKET

KEY FINDINGS

- Whilst the use of social media by these events is relatively new, it has certainly been capitalised upon by them as a means of **communicating with a wider audience**.
- Despite being in competition, each of the 164 trade shows are linked in some way digitally, demonstrating the degree **of interconnectedness their online presence has facilitated**.
- The physical show spaces facilitate a wide-ranging and rapid exchange of information and technical know-how. **They can be thought of as ‘temporary clusters’**.
- Social media and websites have provided a way for this clustering to be year-round and thus more permanent, creating **hybrid-hotspots of intensive exchange of knowledge, new ideas and network building**.

Introduction

Our guiding hypothesis having taken the analysis of Section 3 into account was that such an approach could only provide us with certain, broad, information and that particular hot spots would be context specific in the same way as their more traditional and geographically permanent counterparts (for example Silicon Valley). Therefore, **it does not necessarily stand to reason that the biggest trade fairs in terms of physical size/history are those with the largest impact/influence** and diffusion of promotion.

Thus there we have deployed a two stage digital analysis – **the extent of the network, and its content**. In order to achieve this we firstly had to build a digital corpus that maps the extent of interactions between different actors. Following this we could scrape keywords from these interactions (or interrogate the corpus for specific phrases) to highlight particular knowledge that is being exchanged, and between which actors. Finally, it was necessary to visualise this data to draw conclusions regarding the relative intensity of different hotspots based on the *buzz* they generate (distance of diffusion, intensity of exchange, different actors reached and so forth).

This section outlines tentative early findings based on this principle, flowing into a future framework that will allow a centralised resource to enable us to pinpoint with ease both **what is a hot topic**,

and where the hotspots for promotion can be located. The information we can gather from the dataset extends beyond simple statistics generated from visitor numbers of the year of the first show. By utilising new data mining tools available we can begin to extract information about the relation between the individual events held every year, along with the flows of information between them and where these are situated. It is using this technology that allows us to build a picture of the **trade fair and exhibition sector as far more than simply isolated incidents of economic exchange, but as actual nodal points in the transfer of knowhow about security.**

The open-source tools deployed come from two locations. *Medialab* is based at Sciences Po, Paris. It was founded in 2009 as a centre of research and practice that connects the social sciences with new digital tools with the goal of bringing together a set of knowledge and capacities necessary for the development of a digital humanities. With its technical and methodological expertise, the *Medialab* has become an essential partner in digitally-focused research projects in the human and social sciences. As the day-to-day activity of people and institutions becomes more and more oriented toward the web, the fact that the traces of these activities are easily recoverable using simple digital techniques offers a powerful field of observation for researchers in the social sciences (Medialab 2014). The *Digital Methods Initiative* (DMI) is a contribution to doing research into the "natively digital" (DMI 2014). Put simply, the goal of the DMI is not simply to import well-known methods - be they from humanities, social science or computing. Rather, the focus is on how methods may change, however slightly or wholesale, owing to the technical specificities of new media. In short, the DMI aims to bring together, into a central framework, their expertise developed over a number of years for the purposes of information and data-sharing, teaching and research, in a 'collaboratory' approach. In particular the initiative seeks to invite Internet researchers to think in a precise way concerning the specificity of the new medium and the distinctive approaches to its study. The specific tools used in each case are detailed below.

EXTENT OF THE DIGITAL NETWORK

A large scale visual mapping of the network is one of the best ways to visualise the research completed. Whilst such a map is too large for a document of this format², an excerpt can be seen in Figure 6. This web of interconnections has been built based upon Google's own algorithm for

² Please see the 'Documents' section of the MappingSecurity.net website for a large scale rendering of the map.

cataloguing related and interacting web entities. It partly relies on "similar-to" queries (which uses Google's own algorithm to list websites it believes are related to the original search terms) on Google along with a ranking of search results partly based upon the number and importance of links pointing to a particular page. The nodes displayed are based on Google's database to determine and display the links between a query and other pages on the web.

The results are displayed in a graph that shows both inbound and outbound relationships between nodes. Such a mapping provides an excellent way to visualize networks of interrelated information, rendering it possible to navigate through large networks. The rectangular boxes represent every international trade show and exhibition currently operating worldwide, whilst the circular icons represent other web entities they are connect to. The lines drawn between them represent these interconnections and the flows of information between them. The 'halo' surrounding different points represents its relative importance in terms of the number of interconnections with other points on the graph, as well as the quantity of related information that can be found there. This map demonstrates a number of important points. Firstly, as we can see, the sheer complexity of the interactions and interrelations between the different trade shows is evident, as is their interconnectedness. Only four events are only connected to the rest of the graph by a single point – most have a multitude of intersecting elements that demonstrates they share a certain digital space and move in similar patterns. This is particularly interesting if we consider the vast array of different sectors and geographical locations represented by trade fairs and exhibitions worldwide, and the fact that these events are all more or less in competition with one-another – there is certainly an element of affinity here. Equally as important, particularly if we wish to build a case that these spaces of promotion are themselves a web of information and knowledge exchange that rivals the more traditional security apparatus is the fact that they are *all* connected. Every single node on the graph is related to at least one other. It is possible for information, or indeed a visitor researching a show online, to find their way from one corner of the graph to the other by following the trail of related web entities that connect the points.

CONTENTS OF THE DIGITAL NETWORK

Whilst simply a mapping is in itself is a useful starting point, it does not offer a complete picture – after all if many of the visitors and exhibitors are similar between different events, then a certain degree of online connectedness is to be expected. However, if we look closer at the interactions we can again see that these spaces are engaged in much more than simply economic activity. To do this,

we will focus on the most connected points on the graph, demarcated with the largest halos at the centre of the web, as represented in Figure 6, below. This information has also been drawn from the metadata of the graph to create an easier to visualise wordcloud (Figure 7).

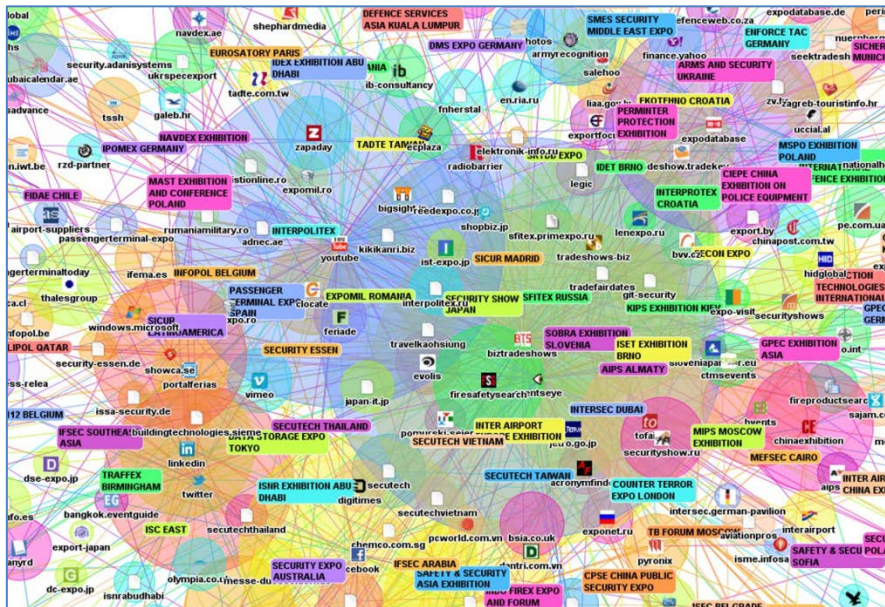


Figure 6 – Close-up of Most Connected Points



Figure 7 - Wordcloud of Most Connected Points

From this information we can see some interesting trends. Some of the most connected points on the graph are the exhibition database websites that have already been discussed in this chapter. This is of no surprise – they are all listed on these sites and they all link to multiple events. The more interesting fact is the next range of hits – Facebook, Youtube, Vimeo, LinkedIn, Twitter are all well represented along with a number of security industry news sites such as sourcesecurity.com. This is an interesting occurrence. Again, one would expect the likes of LinkedIn and Twitter to appear on this graph – after all these are primary mediums for firms to advertise their trade fairs and let people

know of upcoming events. Indeed, as has been discussed these entities help facilitate the lasting connections that are characteristics of a permanent cluster – their social platforms provide exactly the sort of environment to enable the ‘heat-soak’ mentioned previously that can be understood as lasting communication channels that perpetuate and facilitate *buzz* around the events. Similarly, the industry news is likely to report on these events, so their connectedness is to be expected. However, the fact that they are so disproportionately overrepresented on the graph suggests that far more information than simply news of an upcoming event is flowing through these points. Supporting this view is the presence of the likes of Youtube and Vimeo as some of the largest points in the web – these are not the most traditional or easiest ways of disseminating simple ‘when and where’ information about an exhibition, which suggests more is happening here. This is compounded by the absence of technology firms themselves as key nodal points – if all that was happening was simple discussion of events and products then these would be expected to be larger.

SPACES OF PROMOTION AND THE TRANSFER OF KNOWHOW

We can add more nuance to the issues raised above by focussing on the key points of interactions, abstracting the network to the primary sites of interconnectedness of the dataset. This is also an opportunity to deploy a different tool, and thus verify our results are replicated when using different algorithms to assess connectivity. Figure 8, below, has been generated using IssueCrawler, created in Amsterdam. The IssueCrawler is web network location and visualization software. It consists of crawlers, analysis engines and visualisation modules. It is server-side software that crawls specified sites and captures the outlinks from the specified sites. For our purposes here we have conducted a co-link analysis. Co-link analysis crawls the seed URLs (the individual websites of each trade fair and exhibition in our dataset) and retains the pages that receive at least two links from the seeds. The IssueCrawler then has the capability to visualise the results in circle, cluster and geographical maps. A cluster map is represented by Figure 8:

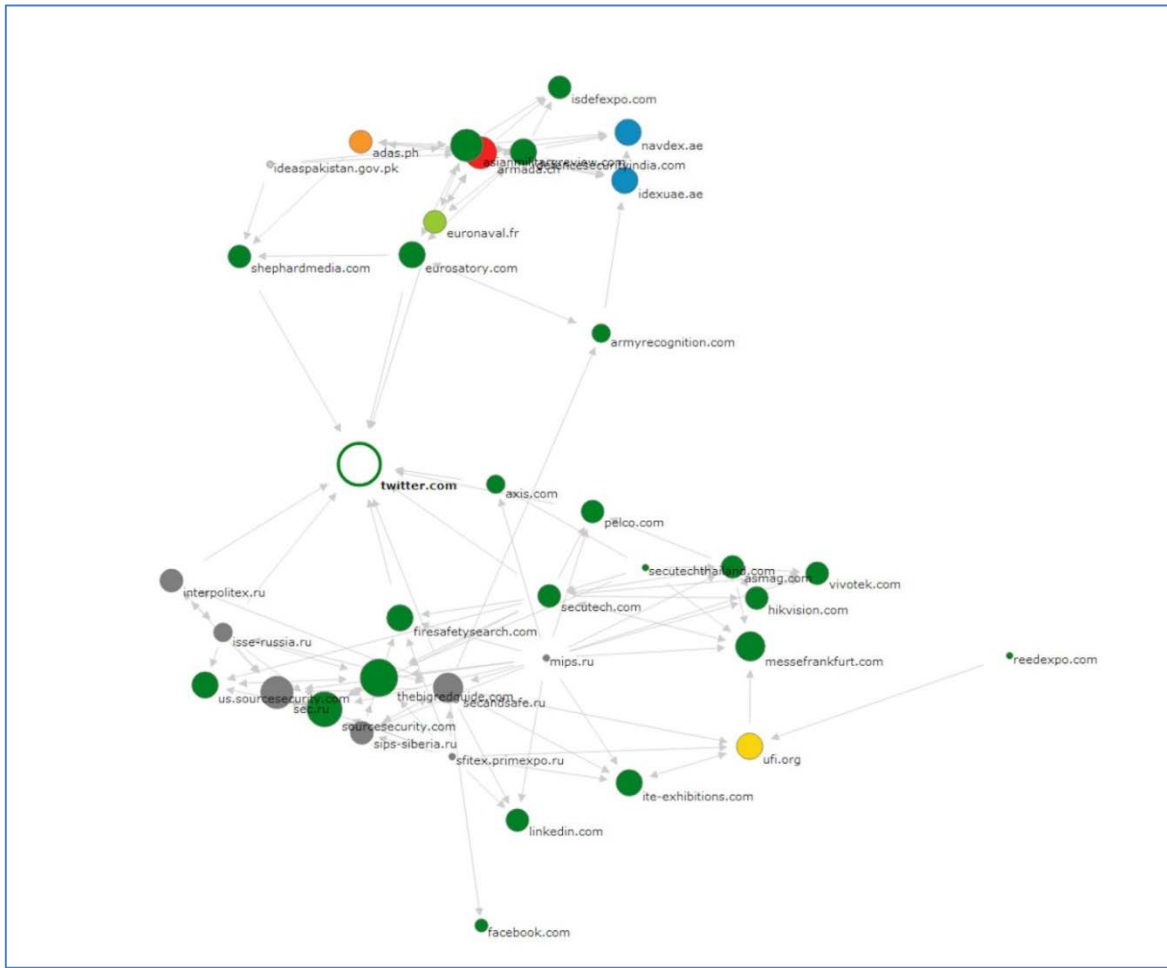


Figure 8 - IssueCrawler Network of Key Sites of Interaction

Again, this confirms the Google based analysis discussed above – we can again see Twitter, Facebook and LinkedIn as key sites that are linked across multiple trade fair and exhibition sites. However, what this also makes clear is a final point of interest here, which is the scale of some of the shows (and their organisers) in terms of their interconnectedness. IFSEC and Reed Exhibitions (two of the largest global security even companies) both feature prominently on the graph (bottom centre of Figure 6, and centre-right of 8, where UFI is IFSEC’s parent company), certainly with a larger halo than their share of global events on their own represent. This suggests they are themselves (at least in terms of their web presence) the sites of, and engaged in, the propagation of more information than simply that related to the trade fairs and exhibitions they run. This is supported by the fact that they are heavily interlinked on Figure 8 with many other trade fairs, despite being supposedly in direct competition with many of them. They are also interlinked with websites such as *armyrecognition.com* which is itself a defence and security technology online magazine - and again

the extent of the interconnectedness suggests there is more information being exchanged here than simply details about the next event being held.

Whilst beyond the scope of this project, there is a feature of IssueCrawler that is worth briefly mentioning here as an additional point of interest and something that certainly warrants further research. The software can construct geographic maps of the locations of the websites of the networks it builds, using a WHOIS search. This can be seen as Figure 9, below:

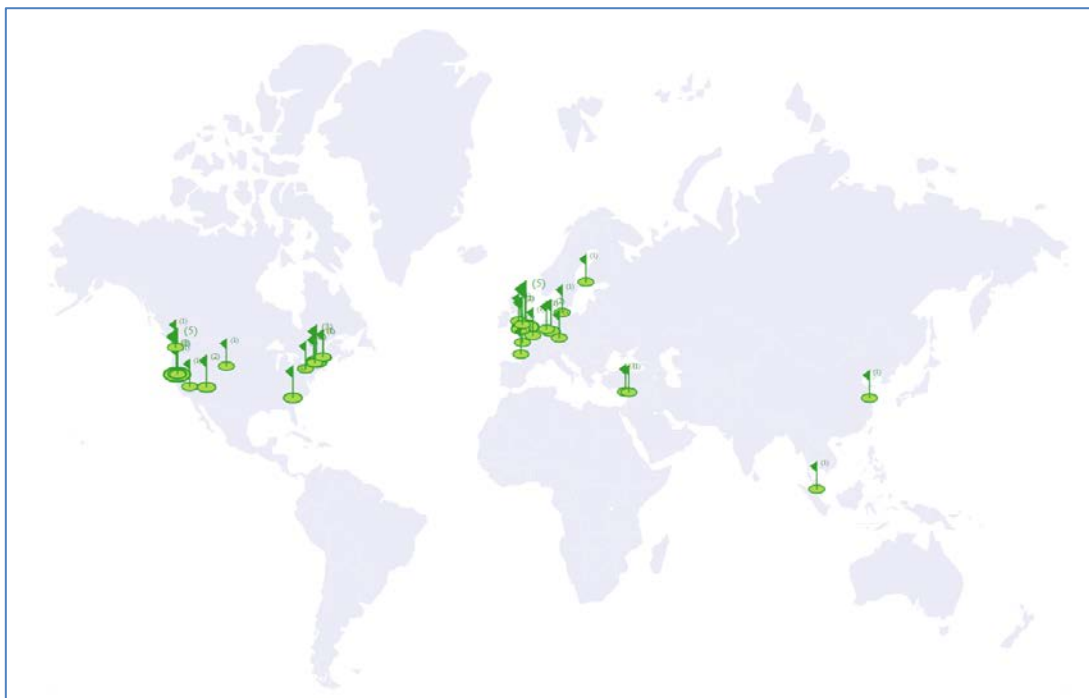


Figure 9 - Geographic Map of IssueCrawler Network

What seems relevant to point out here for future discussion is the way the geographic distribution of important nodal points changes. If we compare the above with Figure 3 this become clear. In Figure 3 we see the importance of European sites in terms of global distribution of events, with a surprising lack in the US. This is primarily a result of US events having a national rather than international focus meaning they do not meet the criteria outlined above for inclusion in this analysis as *international* events (although no doubt worthy of research in their own right). However, this trend is balanced out when we look at the online entities that play an important part here. Whilst Europe is certainly still prominent in Figure 9, there is a strong clustering in the US that cannot be ignored. This represents both the infrastructure of some of the social media platforms being used (Twitter, Facebook and so forth), but also important players in the technology sector itself, suggesting there might well be a stronger US representation and influence that previously thought. This also raises an

interesting question of influence and trend-setting beyond the trade fairs and exhibitions themselves as traditionally conceived. Do the social media platforms that such events use warrant consideration as important players in this process in their own right? After all, the way posts are written and displayed is defined by their rules (140 characters on Twitter, Facebook’s social graph or Google’s ranking algorithm). Furthermore, what does this mean for the influence of certain geographic regions, even if they aren’t as well represented in terms of events themselves - has the move towards hybrid-hotspots begun to redefine what it means to display and discuss such tools in a way that actually *hosting* international events is no longer a requirement for participating in the broader market? These are all important questions that are beyond the scope of this initial project, but which could provide interesting insight and complementary analysis in future work.

However, whilst this discussion is useful as an overview to demonstrate the complexity of the international event sector and its reach, it only gives us a limited indication of what sorts of information is flowing between these points, and the overall influence these events have. In order to look at this in more detail, this working paper will look at ways to quantify exactly what is being exchanged between the different nodes, and ways in which this can be suitably interrogated.

There are two approaches this project has sought to take with regards to quantifying exactly *what* is being discussed within the hot spot. This has taken two forms. The first was to use the Issue Discovery Tool to interrogate the information gathered from the web presence of the trade fairs in order to identify the most relevant keywords and phrases used within it. This initial output can be seen below as Figure 10:



Figure 10 - Issues Discussed

Figure 10 is represented as a wordcloud which attributes a larger font size to those words or issues which appear most often. The goal of this kind of analysis is to be able to track both the current ‘hot topics’ among the actors in the network, but also to trace emerging trends. By taking readings like the one above over a period of time, it will be possible to trace the growth of particular terms or issues and thus chart the rise of emerging trends in the marketplace. For example, we can see that this particular wordcloud highlights *protection* and *equipment* amongst other terms as currently the most discussed or exchanged, however adding a temporal element to the analysis with further investigations will enable a more nuanced understanding of how these discussions develop and become more or less significant over time.

The second process of quantifying the knowledge exchange take place was to be able to interrogate the data for *specific* phrases or topics. This allows not only an analysis of which actors are discussing which phrases, but would allow interested parties and policymakers to question the data to see in which trade fairs and exhibitions particular products or sectors are both most discussed, but also most disseminated amongst the wider network. This would allow for the targeting of particular innovations or research. Such a test-case can be seen below for the phrase “CCTV”:



Figure 11 - Wordcloud of sites most discussing 'CCTV'

Here we can easily see that discussions of ‘CCTV’ are dominated by a relatively small collection of events, with Secutech.com being the most prominent. Secutech (Taiwan) is an event that bills itself as an event specialising in categories including CCTV and digital surveillance. Interestingly for our initial hypothesis is the fact that the event has just short of 26000 visitors and has a relatively short history (running since 1998). Similarly we have Secon Expo (Korea), running since 2000 with 31747 visitors at the last event. Whilst in terms of visitor numbers these can be considered slightly above average (although by no means near the top of the list), what is interesting is that these are events that symbolise the growth of the market both in geographical location terms but also in areas of expertise being put on display. This kind of analysis allows us to see the extent to which the digital is

changing the playing field – whilst it would be expected for CCTV (a run-of-the-mill security tool present at nearly all exhibitions) to have a broad spread of buzz across the network, this shows how it has been capitalised by smaller events outside of the geographic hot spot of Europe, and with much shorter histories than some of the more famous shows. Whilst these trade shows would not be targets based on an analysis of just the dataset discussed in Section 3, new digital methods have highlighted them as key for those with an interest in the promotion of CCTV and related tools.

Whilst the above analysis is only an early output from the tools deployed as part of this study, it demonstrates the value and nuance such a quali-quantitative digital study can bring, particularly when taken in conjunction with a more traditional mapping.

5. CONCLUSIONS

By offering a first original mapping of the wider expansion and logic of the security fair world into the digital domain, and a detailed consideration of *who* and *what* is being discussed, HOSSET has made it possible to develop a better understanding of both the makeup and relations between these elements, enabling us to identify both emerging trends in the marketplace and the hotspots which act as the primary conduits for such developments. Although our preliminary results are mostly anecdotal at this stage, this report has shown that the tools and techniques used demonstrate the potential to add valuable insight into future research into this marketplace, as well as an excellent way to provide horizon-scanning capabilities for parties with interests in specific market areas beyond academic concerns. Thus, our recommendations, needs and future trajectories going forward can be summarised as:

- To continuously **update a knowledge base** of international security trade fairs and trade shows;
- To **chart the technologies** of anticipation, prevention and risk management deployed by these professional networks and institutions involved in securing our Western societies;
- To further **develop a set of research principles and methodologies** for surveying and documenting security professionals and trade fairs involved in the provision of high tech security;
- To build this development into something **accessible and open-source** that can be utilised by a wider audience;
- To contribute to critical reflection on the **transformation of security and impact on societal cohesion** and political decision processes.

REFERENCES

- Amoore, L. (2007) 'Vigilant Visualities: the Watchful Politics of the War on Terror,' *Security Dialogue* 38(2): 215-232.
- Amoore, L. and M. De Goede. 2008. *Risk and the War on Terror*. Padstow: Routledge.
- Anderson, B. (2010) 'Security and the Future: Anticipating the event of terror,' *Geoforum* 41:227-235.
- Aradau, C. and R. van Munster (2011) *The Politics of Catastrophe: Genealogies of the Unknown*. London: Routledge.
- Bathelt, H. & N. Schuldt (2010) 'International Trade Fairs and Global Buzz, Part I: Ecology of Global Buzz,' *European Planning Studies*, 18:12, 1957-1974
- Bathelt, H. & Schuldt, N. (2008) 'Between luminaires and meat grinders: International trade fairs as temporary clusters,' *Regional Studies*, 42(6), pp. 853–865.
- Bathelt, H., Malmberg, A. & Maskell, P. (2004) 'Clusters and knowledge: Local buzz, global pipelines and the process of knowledge creation,' *Progress in Human Geography*, 28(1), pp. 31–56.
- Bigo, D., Jeandesboz, J., Martin-Maze, M and F. Regazzi, (2014) 'Review of security measures in the 7th Research Framework Programme FP7 2007-2013,' *Study for the LIBE Committee*, European Parliament.
- C.A.S.E Collective. (2006). "Critical Approaches to Security in Europe: A Networked Manifesto," *Security Dialogue* 37(4): 443-487.
- Cornish, P. (2010). 'Technology, Strategy and Counterterrorism,' *International Affairs* 86(4): 875-888
- Digital Methods Initiative, (2014). 'About,' DMI Website (<https://wiki.digitalmethods.net/Dmi/DmiAbout>) [Accessed 7/7/14]
- Ericson R. and D. Haggerty. (1997). *Policing the Risk Society*. Toronto: University of Toronto Press.
- Garland, D. (2001). *The Culture of Control*. Oxford: Oxford University Press.
- Guttet E.-P., Jeandesboz J. (2009). 'Security technologies', in P. Burgess (Ed.), *Handbook of New Security Studies*, London: Routledge: 229-239
- Loader, I. and N. Walker. (2007). *Civilising Security*. Cambridge: Cambridge University Press.
- Loader, I. (1999). Consumer culture and the commodification of policing and security. *Sociology*, 33(2), 373-392
- Malmberg A, So Ivell Ú, Zander I, (1996), "Spatial clustering, local accumulation of knowledge and firm competitiveness" *Geografiska Annaler* 78B: 85-97

Malmberg A, (1996), "Industrial geography: agglomerations and local milieu" *Progress in Human Geography* 20: 392-403

Malmberg, A and Maskell, P. (2002). "The elusive concept of localization economies: towards a knowledge-based theory of spatial clustering," *Environment and Planning A* 34, 429-449

Marshall A, (1920) *Principles of Economics* 8th edition (Macmillan, London)

Maskell P, (2000), "Social capital and competitiveness", in *Social Capital: Critical Perspectives* Eds S Baron, J Field, T Schuller (Oxford University Press, Oxford) chapter 6, pp111-123

Maskell P, Eskelinen H, Hannibalsson I, Malmberg A, Vatne E, (1998). *Competitiveness, Localised Learning and Regional Development: Specialisation and Prosperity in Small Open Economies* (Routledge, London)

Maskell, P, H. Bathelt & A. Malmberg (2006) 'Building global knowledge pipelines: The role of temporary clusters,' *European Planning Studies*, 14:8, 997-101

Maskell, P, (1998), "Successful low-tech industries in high-cost environments: the case of the Danish furniture industry" *European Urban and Regional Studies* 5: 99-118

Medialab. (2014), 'About,' Medialab Website (<http://www.medialab.sciences-po.fr/about/>) [Accessed 7/7/14]

Nesta. (2013), 'Joining the Dots: Can events grow networks of innovators?,' Nesta Website (<http://www.nesta.org.uk/blog/joining-dots-can-events-grow-networks-innovators>) [Accessed 2/10/14]

O'Reilly, C. (2010). 'The transnational security consultancy industry A case of state-corporate symbiosis.' *Theoretical Criminology*, 14(2), 183-210

Porter M E, (1994). "The role of location in competition" *Journal of the Economics of Business* 135-39

Porter, M. E. (1990): *The Competitive Advantage of Nations*. New York: Free Press.

Porter, M. E. (1998): Clusters and the new economics of competition. *Harvard Business Review* 76 (November-December): 77-90.

Rubalcaba-Bermejo, L and J Cuadrado-Roura. (1995). "Urban Hierarchies and Territorial Competition in Europe: Exploring the Role of Fairs and Exhibitions" *Urban Studies* 32: 379-400

Sabel C F, (1989), "Flexible specialisation and the re-emergence of regional economies", in *Reversing Industrial Decline? Industrial Structure and Policy in Britain and her Competitors* Eds P Hirst, J Zeitlin (Berg, Oxford) pp 17-70

Scott A J, (1998), "From Silicon Valley to Hollywood: growth and development of the multimedia industry in California", in *Regional Innovation Systems: The Role of Governances in a Globalized World* Eds H J Braczyk, P Cooke, M Heidenreich (UCL Press, New York) pp 136-162