Handbook on Networks in Innovation and Crisis Management: Theory and Practice in a Dynamic and Disruptive Environment

Volume 2: Social Value Creation in Dynamic Networked Situations

Edited by
Roland Ortt
Claudia Bücker
Stefan Klein

Delft, Leiden, Münster 2016
Handbook on Networks in Innovation and Crisis Management:
Theory and Practice in a Dynamic and Disruptive Environment

Volume 2: Social Value Creation in Dynamic Networked Situations

Edited by
Roland Ortt
Claudia Bücker
Stefan Klein

Delft, Leiden, Münster 2016

DOI: 10.17879/64219709075
http://dx.doi.org/10.17879/64219709075

URN: urn:nbn:de:hbz:6-64219710246
http://nbn-resolving.de/urn:nbn:de:hbz:6-64219710246

Open access is granted under the CC BY-ND-3.0 license
(http://creativecommons.org/licenses/by-nd/3.0/).

Research for this handbook has been funded within the Marie Curie Research & Innovation Actions by the European Union’s Seventh Framework Program FP7/2007-2013 under REA grant agreement n° _317382, NITIMesr.
Volume 2: Social Value Creation in Dynamic Networked Situations

Introduction to the volume

This volume serves as a forum for researchers and partners with an interest in social value creation in dynamic networked situations. It brings together scholars (and practitioners) from several disciplines and practices that want to understand social value creation: reactions of a network to disasters, and prevention of possible disasters within these networks. To that end they study various contexts such as the epidemic diffusion of a cyber crisis, the identity management to increase cyber security and the use of social media by the police to gather information and coordinate in case of disasters. This volume has theoretical roots in a variety of theoretical perspectives and disciplines such as diffusion modelling, IT security management and communication sciences.

The editorial team
Roland Ortt
Claudia Bücker
Stefan Klein
# Table of Content Volume 2

## Volume 2: Social Value Creation in Dynamic Networked Situations

### Table of Content Volume 2

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Review of Epidemics Modeling Approaches to Understand Cyber Crises</td>
<td>1</td>
</tr>
<tr>
<td>Abstract</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Method</td>
<td>3</td>
</tr>
<tr>
<td>Deterministic and stochastic models</td>
<td>4</td>
</tr>
<tr>
<td>Networks and Spatial models</td>
<td>11</td>
</tr>
<tr>
<td>Computational epidemiology</td>
<td>22</td>
</tr>
<tr>
<td>From epidemiology to cyber epidemics modeling</td>
<td>24</td>
</tr>
<tr>
<td>Discussion</td>
<td>29</td>
</tr>
<tr>
<td>References</td>
<td>30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Brief Introduction to the Emergency Service Sector</td>
<td>35</td>
</tr>
<tr>
<td>Introduction</td>
<td>35</td>
</tr>
<tr>
<td>A Brief History of the Emergency Services</td>
<td>36</td>
</tr>
<tr>
<td>Contemporary Organizational Structures of the Emergency Service Sector</td>
<td>45</td>
</tr>
<tr>
<td>Collaboration and Integration in the Emergency Service Sector</td>
<td>48</td>
</tr>
<tr>
<td>Conclusion</td>
<td>51</td>
</tr>
<tr>
<td>References</td>
<td>53</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literature Review: Identity Management, Cyber Security and Crisis &amp; A Case Study on IdM System Adoption</td>
<td>56</td>
</tr>
<tr>
<td>Introduction</td>
<td>56</td>
</tr>
<tr>
<td>Definitions and Basics</td>
<td>57</td>
</tr>
<tr>
<td>Identity and Access Management Systems</td>
<td>61</td>
</tr>
<tr>
<td>Architectural models</td>
<td>63</td>
</tr>
<tr>
<td>Paradigms of IdM systems</td>
<td>67</td>
</tr>
<tr>
<td>Crisis situations and challenges in IdM</td>
<td>68</td>
</tr>
<tr>
<td>Case study: Forgerock as Identity Management System for eGovernment Service - Bürgerservice-Portal</td>
<td>72</td>
</tr>
<tr>
<td>The Project Structure</td>
<td>76</td>
</tr>
<tr>
<td>Stakeholder presentation and stakeholder analysis</td>
<td>77</td>
</tr>
<tr>
<td>Conclusion</td>
<td>89</td>
</tr>
</tbody>
</table>
A Review of Epidemics Modeling Approaches to Understand Cyber Crises

Elisa Canzani

Abstract

Epidemiology represents a solid research field that has attracted a wide range of mathematicians and modelers contributing in the area of public health and disease management. Over the years, approaches and techniques from epidemics modeling have been adopted to explore diffusion phenomena of social, innovation and communication systems. Modeling complex dynamics of cyber crisis situations is a particular research interest that strongly motivated this work. Accordingly, this article provides an overview of mathematical insights emerging from epidemiological research patterns, to discuss how epidemics models have been inspiring research in the cybersecurity domain. References to comprehensive reviews, pioneering and most relevant results in biological and cyber epidemics modeling are given with the attempt to guide rational decisions in choosing models for applications.

Introduction

Modeling epidemics spread has attracted the interest of many researchers over the years, and epidemiology constitutes a solid branch of the literature in understanding transmission characteristics of infectious diseases that can lead to better approaches to decreasing their transmission in communities, regions and countries. Obviously, real experiments are impossible or unethical in the context of epidemics such as in any other disaster or crisis situation. (For more details on why to do epidemiologic modeling see Hethcote [1]). Nevertheless, decision-making tools need underlying knowledge of complex dynamics of crises. The lack of understanding of crucial factors influencing the dynamics’ spread of infectious diseases often turns into failures of vaccination strategies or inability to quickly react in such crisis situations. How to capture such nonlinear behaviors by identifying different causes of epidemics diffusion is one of the major concerns of epidemiology.

One of the public health’s greatest victories is the eradication of smallpox in 1977, and the first modeling contribution for infectious diseases refers exactly to this tremendous virus that has
spread around the world from the earliest civilization until the 20th century [2]. It was only in 1766 when a physician, Daniel Bernoulli, formulated a mathematical model to evaluate the effectiveness of a certain vaccination against smallpox [3]. One milestone in modeling epidemics is the model of Ross [4] for the transmission of malaria. Later, a couple of seminal works established the basis of the current trends in mathematical epidemiology. Among them, it is definitely worth mentioning the general and rigorous study made by Kermack and McKendrick [5] that refers to the SIR epidemic model. These studies demonstrate not only the variety and expressiveness of mathematical models but also their contribution to understanding transmission and finally to developing successful intervention strategies.

However, epidemiology as discipline has emerged only in the 20th century, when mathematical modeling of epidemics has become important to address theoretical gaps that may lead to practical consequences related to public health. Arguments for the utility of mathematical methods in public health can, e.g., be found in [6]. Modelers and mathematicians have been strongly contributing to understand the “persistent threat” of epidemics by developing “more than a thousand and one” epidemiological models [7]. Hundreds references can be found in the SIAM review on the mathematics of infectious diseases [8]. With the exception of the SIAM review, several reviews articles highlight a substantial lack of guidelines which focus on modeling approaches to epidemiology rather than in understanding the dynamic diffusion of a particular virus. A comprehensive survey of mathematical models (mainly differential equation based) for the transmission of Malaria was recently carried out by Mandal et al. [9]. The review elaborates on evolution of modeling strategies by using some key models, but does not abstract from referring to a specific pathogen. The seminal work of Diekmann and Heesterbeek [10] on modeling patterns and reviews, in chronological order, the main highlights by explicitly naming ‘actors’ and places that have been involved in the modeling and analysis of epidemics. On the basis of these pioneering works, mathematical epidemiology seems to have exponentially grown from the middle of the 20th century.

Improved sanitation and vaccination programs have succeeded in controlling some epidemics, but biological agents adapt and evolve so that new infectious diseases have emerged and some existing diseases have reemerged. The etiological agent for AIDS (i.e. HIV) emerged in 1981 and it is nowadays an important sexually transmitted disease throughout the world. Plague, cholera and hemorrhagic fevers such as Ebola continue to erupt occasionally. Recent advances in epidemiology apply existing models to these agents and their recent threats [11]–[13].

Our research interest is this dynamic modeling of crisis situations, with a special emphasis on cyber crises. We refer here to the stream of literature on the spread of biological agents on the one hand and on the literature on the spread of computer malware. The metaphors of virus and
infection are used in the IT-domain for the effects of malware, its spreading and effects. As the stream of literature that discusses models and methods to address cybersecurity and critical infrastructures protection is more recent and limited when compared to the extant stream of literature in epidemiology, epidemics modeling can be naturally considered a related field to get knowledge on computer viruses spread dynamics.

This article focuses on main modeling approaches and mathematical insights emerging from these models. In line with Hethcote [7], we believe applications of results of epidemics models are significantly behind the mathematical theory rather than in papers modeling specific diseases. Our goal is to review the literature on the (mathematical) models, the questions that they can answer and the insights gained from modeling on the dynamics of crisis situations.

Accordingly, the contents are organized on the basis of five patterns we identified for epidemiology modeling. They range from the early contributions of deterministic and stochastic models (Section 3) to network and spatial models (Section 4) that incorporate dynamics of interacting elements. The growing recognition that multilevel factors may influence health and disease has led to the adoption of new modeling technologies, that is to the rise of computational epidemiology (Section 5). Then, applications of biological research to current crisis situations affecting the cyber world are presented (Section 6). The chapter concludes with a final discussion on valuable contributions and some limitation of biological and epidemics models applied to new field of computer security, currently dealing with the understanding of complex cyber epidemics and networked systems recovery from tremendous cyberattacks (Section 7).

**Method**

With this purpose, an extensive literature review was performed through an electronic search of academics databases on the Internet (e.g. Science Direct, Elsevier, Google Scholar, ACM digital library, Springer link etc.). Guidelines followed to structure the review refer to Randolph [14] and Webster [15].

Our evident focus on research methods and the wide range of existing epidemic models led to a qualitative literature review which look for pivotal articles in the field. Overall, we looked for seminal reviews and most cited papers that analyze models breaking new grounds or showing important new aspects. Hence, a snowball approach allowed assessing the relevance of selected articles.
This literature analysis comprises two rounds. The first round was to identify the core epidemiological research on modeling epidemics. Accordingly, the data collection process was done on the basis of specific key words, such as “crisis dynamics”, “crisis modeling”, “epidemic models”, “mathematical epidemiology”, “modeling infectious diseases”, and combinations of them. A well-rounded collection of articles has been identified and a preliminary work has been published in the proceedings of ISCRAM 2015 (See [16]). For this first round the literature search in the databases was conducted in November 2014 and snowballing continued until February 2015.

Then, a second round of literature review was performed according to the authors’ interest in understanding how such epidemics models have facilitated research towards the emerging field of cyber crisis modeling. Here, interesting articles were collected in a snowball approach using additional key words related to the cyber world. In particular, a comprehensive body of literature has been identified by combining key words such as “computer” or prefix as “cyber-” with biological-inspired terms (i.e. “epidemics”, “virus”, “immunology”, etc.) and more technical words such as “mathematical modeling”, “crisis dynamics”, and “diffusion process”, already used in the first round of literature analysis. The search for this second round was conducted in March 2015 and snowballing continued until April 2015.

**Deterministic and stochastic models**

The earliest epidemic model dates back to 1760. It has been developed by Daniel Bernoulli to show that the life expectancy could be increased by a universal inoculation against Smallpox [3]. In the early 1900, Ross published series of papers using mathematical functions to study the transmission of Malaria [4]. However, modern mathematical epidemic modeling is considered to have started with McKendrick and Kermack. In 1927, they formulated a simple deterministic model that was successful in predicting the behavior of outbreaks if applied to many recorded epidemics [5]. Mathematical insights of their model are explained later on in this document.

Overall, the model assumes that only susceptible individuals can get infected and, after having been infectious for some time (infectious period), an individual dies or recovers and becomes completely immune hereafter. Real situations are far away from the scenario described above, but studies on such simple model led to the earliest milestone in epidemiology modeling: the McKendrick-Kermack threshold condition. It states that an infection outbreaks if and only if $R_0 > 1$, where the basic reproduction ratio $R_0$ is defined as the average number of secondary infections produced when one infected individual is introduced into a fully susceptible host population.
However, this conceptual result was also based on the restrictive assumption of a ‘close’ community, i.e. without births, deaths, immigration and emigration during the study period. The threshold quantity $R_0$ was studied over the years in more general deterministic models and under more realistic conditions. More details on the role of $R_0$ can be found in [8].

Often, deterministic epidemiology modeling refers to the so-called ‘compartments models’. Compartments represent the epidemiological categories in which individuals are divided when a pathogen appears in a community. A general standard notation labels such classes with $M$, $S$, $E$, $I$, and $R$, as it is shown in a general transfer diagram in the figure below.

![The general transfer diagram for the MSEIR model [8].](image)

The class $M$ contains the infants born with passive immunity, in $S$ there are susceptible individuals that can move in the class of exposed $E$ if they are in the latent period after they get infected. Then, the individuals enter in the class $I$ of infectives when the latent period ends, and finally $R$ is the class containing those who recover from the infection and have acquired a permanent immunity. Note that for models assuming a close community, and then without deaths, $R$ stands for “removed”, which are individuals either recovered and immune, or dead.

As for the MSEIR model in Figure 1, note that acronyms for epidemic models are often based on the flow patterns between compartments. In general, the partition (i.e. which compartments to consider and in which order individuals can transfer from one to another) depends on parasite density inside individuals and the type of infection. For instance, diseases transmitted by bacteria usually have no immunity against reinfection, and the terminology SIS is used to indicate that the passage of individuals is from the susceptible class to the infective class and then back to the susceptible class. Diseases transmitted by viral agents confer immunity against reinfection and they have different compartmental structure from diseases without immunity. This is the case of Smallpox, described by McKendrick and Kermack with the SIR epidemic model in which individual can only move from $S$ to $I$ and from $I$ to $R$.

Mathematically, compartmental models are formulated as a set of differential equations. Given the time $t$ as independent variable, the rates of transfer between compartments are expressed
as derivatives with respect to time of the compartments’ sizes. Referring to McKendrick and Kermack, the first SIR model was based on the following assumptions:

1. Given a close and large population of size $N$, $S(t)$, $I(t)$, and $R(t)$ are the numbers of individuals in the respective classes such that $S(t) + I(t) + R(t) = N$ at time $t$;
2. Let $\beta$ the constant contact rate, an average member of the population makes contact sufficient to randomly transmit infection with $\beta N$ other individuals per unit time;
3. The quantity $1/\gamma$ is the average infectious period so that infectives leave the class I with a rate of $\gamma I$ per unit time.

The SIR model was defined as an initial value problem as follows:

$$\frac{dS}{dt} = -\frac{\beta I S}{N}, \quad S(0) = S_0 \geq 0,$$

$$\frac{dI}{dt} = \frac{\beta I S}{N} - \gamma I, \quad I(0) = I_0 \geq 0, \quad (a)$$

$$\frac{dR}{dt} = \gamma I, \quad R(0) = R_0 \geq 0.$$

Obviously, a homogeneous uniformly mixing community (1.), a rate of contacts proportional to population size $N$ with constant of proportionality $\beta$ (2.), and an exponentially distributed recovery rate (3.) are unrealistically assumptions. However, this illustrates that important conceptual results can be deduced from extremely simple models.

Simple mathematical manipulations can prove that the quantity $\beta S(0)/\gamma$ is the basic reproduction number $R_0$ previously introduced in this document. The so-called Threshold Condition states that when $R_0 > 1$ the epidemic spreads affecting a substantial fraction of the population, and when $R_0 < 1$ no epidemics can occur. In particular, if $R_0 = 1$ a disease is maintained in a population and the situation is referred to as being the ‘endemic state’ (See [17] for the problem of endemicity). The two very different scenarios separated by this critical value are shown in Figure 2, where $(S(t), I(t), R(t))$ are plotted over time.
This dichotomy refers to solutions of the system of differential equations (a) having initial configuration $S_0 = 0.99, I_0 = 0.01$ (to the left is the case with $R_0 = 1.5$ and to the right with $R_0 = 0.5$). Thus, the equations (a) can be used to obtain a balance equation for the final size of the epidemic $z$, i.e. the fraction of population that at the end of the epidemic was infected. In Figure 3, the solution $z$ is plotted as a function of the threshold value $R_0$ assuming that the initial fraction of infectives $I_0$ approximated to 0.

However, results rely on the assumption of a homogeneous uniformly mixing community that may not be suitable in some real cases. For instance, not always the time scale of the disease is much faster than the time scale of births and deaths so that demographic effects on the population can be ignored as the hypothesis (1.) implies. Moreover, it is generally difficult to estimate the contact rate $\beta$ since it may also depend on social and behavioral factors.

In general, in formulating models as differential equations it is assumed so far that the epidemic process is deterministic. This means that the behavior of a population is completely determined by its history and by the rules describing the model. Questions typically addressed with
Deterministic models are: when an epidemic outbreaks? How many individuals will get infected if the epidemic takes off?

As problems were solved, simple models were generalized through more realistic extensions. The main generalization of the initial deterministic epidemic model was to study stochastic epidemic models. A survey paper with interesting references on stochastic epidemic modeling is [19]. They allow to raise additional questions, for example: what is the probability of a major outbreak?

Stochastic models are surely preferred for considering small communities, in which it seems reasonable to assume some uncertainty and randomness in the final number of infected. In mathematical terms, stochastic models are formulated as Markov chains, and they mainly enable to consider standard errors in estimating parameters from real data of a disease spread. Thus, starting from the original and simplest SIR model, wide ranges of compartmental models, both deterministic and stochastic, were formulated for studying infectious diseases occurred over the years. Models’ extensions were investigated together with the different roles of the threshold value, as multilevel factors affecting dynamics of diffusion do influence the basic reproduction number $R_0$.

A major aspect taken into account by later contributions is the demography of a population, allowing for such features characterizing the so-called ‘dynamic’ community. When natural births do not balance the deaths (in case of significant diseases-related deaths), immigration inflows and emigration outflows are not balanced, and generally when the time period is not very short, the epidemic model must take into account a varying population size. This can be done considering an extension of the simple SIR model which includes also the births class B which changes according to the variation in age distribution of the total population over time. Demographic models describe changing size and mortality rate of a population over time, and therefore they underlie age-structured epidemic models that are discussed below in this document. (Further details on demographic models can be found in [8]).

While early mathematical contributions to epidemiology generally modeled the contact process by the law of mass action, which asserts that the infection is proportional to the term $I(t)S(t)$ in (a), later epidemic models consider that in real life the contact rate depends on the particular disease being studied as well as on social and behavioral factors which characterize different types of individuals.

As a consequence, much of the research in mathematical epidemiology in recent years focused on various types of heterogeneity in transmission of infectious agents within a community (and also between communities).
Realistic epidemic models consider the age structure of a population because risks of an infection can be related to age, the recovered fraction usually increases with age, and vaccination programs often focus on age. Hence, age-dependent mixing models include both time \( t \) and age \( a \) as independent variables [8].

Referring to the SIR model explained above, age dependency in transmission can be easily by replacing the force of infection \( \lambda(t) = \beta I(t) \), i.e. number of contacts that result in infection per susceptible individual per unit time, with a more general function \( \lambda(a, t) \). In this case the force of infection is a composite parameter denoting the sum rates of contact of susceptibles within a given age class with infectious individuals of all age classes.

As a matter of the fact, the diagram below shows that the force of infection for infectious diseases such as the measles virus is strongly age-depended.

![Age-dependent forces of infection for the measles virus in developed countries][20]

Note that the concept of reproductive rate, and then the threshold density of susceptibles \( R_0 \), requires modifications when mixing and contact depend on age. (For more details refer to [20]).

From 1981, when the human immunodeficiency virus (HIV) has become an important sexually-transmitted disease (STD) throughout the world, modeling efforts focused on heterogeneity mixing in sexual behavior. First models assumed that the rate of infection is determined by the probability of transmission per partner contact, times the mean rate of acquiring new sexual partners, times the proportion of infectious persons in the sexually active population [21]. A more general approach considers a stratification of the population based on their rate of sexual partner change.

A qualitative understanding of how variability in sexual activity influences the magnitude of epidemic is provided by May and Anderson [22] in Figure 5. Considering a population of
homosexuals males, they have plotted $I$ in function of $R_0$ for various values of the coefficient of variation ($CV$) in heterogeneous mixing to show that the epidemic essentially “burns” itself out in the highly sexually active groups, while the low activity classes become larger as the heterogeneity is more pronounced.

![Graph showing the fraction of infected I during an epidemic as a function of the basic reproductive number $R_0$, which varies for different levels of heterogeneity (coefficient of variation CV) [22]](image)

The emergence of AIDS highlights the variability in sexual behavior as a dominant feature of pattern of spread and persistence of infection. However, Anderson [20] states that a random mixing weighted by sexual activity is still a crude assumption that would need to consider the proportions of sexual partnerships made by individuals in a given activity group with the ones in other classes. Substantially, such issue turns in a call for ‘networks’ of sexual contacts which define “who mixes with whom”. Also, Anderson [20] notices that analogue considerations are done for the age-structured models.

Before dealing with the important branch of network epidemiology (next section), the discussion on deterministic and stochastic models concludes referring to HIV/AIDS infections. Akpa and Oyejola [23] provide an introduction and a rich mathematical review which focus mainly on deterministic models developed for HIV transmission dynamics and AIDS epidemics. They state that the main limitation of deterministic models lies in taking no account of the randomness of variables or that of all risk factors. However, approximating what happens on average at the population scale, they require less data.

Stochastic models take a different approach as they assume that the response variables are a family of random variables indexed by time so that the epidemic is basically a stochastic process, and then it allows to consider uncertainly and bias into models. As they incorporate chance and provide confidence intervals on result, stochastic models are often more complicated than the corresponding deterministic ones and do not lend easy explanation of epidemic dynamics. A comprehensive study of stochastic epidemic modeling that refers to HIV pathogenesis is provided by Wan-Yuan [24]. Newman states that in recent years the research on traditional epidemics
modeling seems to be exhausted [25], and the field of epidemiology has been revolutionized by the relatively new science of networks. He observes that the models assuming a fully mixing population can be elaborated in sense of the effects of age structure and population turnover, however the crucial element that all such models lack is a network topology. To this concern, Newman has shown that a large class of standard SIR models can be solved exactly on a wide variety of networks.

The following section focuses on modeling efforts that highlight the interplay between network theory and dynamics of epidemics’ spread.

**Networks and Spatial models**

The assumption of fully mixed population is primarily made to allow modelers to utilize differential equations (see (a)) for the so-called traditional models, but it is obvious that in a real situation a given infective individual does not have the same probability to infect all the others [25].

Although many modifications to the basic SIR framework (see previous section) have been made by modeling different mixing rates between population subgroups (that often refer to the so called ‘metapopulation models’), Keeling and Eames [26] point out that the approximation of random mixing remains at least between individuals within each pair of subgroups.

Considering a network topology into epidemic models allows an accurate representation of real contact patterns, which can depend on spatial and geographic components (e.g. for airborne and vector-borne diseases), host-pathogen biology, sexual relationships (such as for AIDS and other sexually transmitted diseases) or several social factors of influence.

Mathematical theory of diseases spread on networks traces back to the mid-1980s with the rise of AIDS\HIV worldwide. First pioneering studies in this context were performed by May and Anderson [22] and Klovdahl [27]. Then, the recognition that connections between individuals, that allow an infectious disease to propagate, naturally define a network has grown rapidly through the years.

Research patterns that have been relating network topologies to diseases dynamics are discussed in this section. Three comprehensive review works were selected ([26], [28], [29]) to provide a description of the most relevant mathematical results in the field.
Overall, historical study of networks has its grounding in two disparate fields: social sciences and graph theory. Basically, the transfer of ideas between these fields and epidemiology can be seen as a matter of vocabularies. While social literature refers to ‘actors’ and ‘relations’, graph theory uses the terms ‘nodes’ and ‘edges’, epidemiology deals with ‘individuals’ and ‘contacts’ [26].

Social network analysis focuses more on how the connections between individuals change according to the rules of social dynamics, than on network structures and proprieties. In contrast, graph theory provides an elegant formalism capable to mathematically describe networks (or graphs) on the basis of the semantic works of Erdös and Renyi in 1950s [30]. Matching both perspectives provides a valuable framework to investigate mixing networks in epidemiology.

Researchers were initially concerned to gather data for determining the sampled network that would have described the real diffusion dynamics of a disease. However, it is easily understandable that several difficulties occur during the data collection process. While using a population approach to define mean field models based on average data (see previous section) is straightforward, trying to trace a real network of individuals within a host population to completely describe the diseases spread requires deep knowledge at individual level.

For such a purpose, three main techniques have been used according to Mossong, Beutels, Auranen, Mikolajczyk, and Edmunds [31]:

- **Infection tracing** to build a transmission network consisting of all the directional links from infected individuals to whom they transmitted the disease so that they are tree-like networks.
- **Contact tracing** to identify a contact network with all potential transmission contacts between individuals, in particular this is the case of STDs for which partner relationships are traced.
- **Diary-based tracing** allows to gather detailed information by recording contacts as they occur, and then the work load is so shifted from the researcher to the subject. Currently, POLYMOD is the most comprehensive diary based study [31].

An alternative source of information comes from the recorded movements of individuals. Four main forms of movement network have been modeled to understand the spread of infectious diseases: the airline transportation network [32], the movement of individuals to and from work, the movement of dollar bills (from which the movement of people can be inferred)[33], and the movement of livestock. A spectacular example of the latter is the Cattle Tracing Scheme containing information of all the movements of all cattle between farms in Great Britain [34].
Mapping spatial heterogeneity in infectious diseases has attracted the interest of many researchers, so that *Spatial Epidemiology* has arisen as the principal scientific discipline to study spatial variations in disease risk or incidence [35]. We return to spatial network models at a later stage in this section.

In general, the tracing method applied depends on the purpose for which the data were retrieved and on the resource available. In any case, data collection processes strictly rely on assumptions, protocols, and participation of individuals in being asked about personal information. As a consequence, the lack of proper information turns in several limitations of the network being sampled.

For this reason, many examples of simulated networks are being developed to match available data on observed social characteristics. Halloran et al. [36] address the most difficult problem by generating a network model for the Smallpox outbreak that takes into account social interaction within households and family groups. Nevertheless, simulations of sampled networks do not allow gaining a proper understanding of the subject matter. Theoretical constructs are needed to effectively understand complex dynamics of diffusion. Developing idealized networks has revealed such network elements, structures and propeties for which definitions were missing. Many mathematical networks have been interest of epidemiologists because they formally describe how individuals are distributed in space (social or geographical) and how relations are formed, making simpler and explicit the “complex rules” of individuals’ mixing.

Continuing the discussion on models for HIV transmission in communities of homosexual males, Anderson [20] provides first examples on how social behavior observation and mathematical tools converge in generating contact networks. The overall idea is to define an adjacent matrix $P$ that determines the population mixing.

The mixing probabilities $p_{ij}$ have a series of constraints as follows. For all $i, j$ combinations,

\begin{align*}
0 & \leq p(i, j) \leq 1 \quad \text{(b.1)} \\
\sum_i p(i, j) & = 1 \quad \text{(b.2)} \\
p(i, j) & = p(j, i) \quad \text{(b.3)}
\end{align*}

Considering that each element $p(i, j)$ describes the proportion of the contacts of an individual $i$ with an individual $j$, the first two properties are trivial. The third one states that connections are symmetric, as infection can pass either ways across a contact in most mixing networks. Shifting such idea to the concept of sexual activity classes, which strongly influence the magnitude of STDs spread, this property affirms that a class $i$ cannot have less or more sexual contacts with
class $j$ than class $j$ can have with class $i$. As a consequence, high activity classes are characterized by a higher mortality rate than the low activity classes.

Thus, distribution of sexual activity will change through time according to the mixing matrix $P$ in which elements satisfy (b.1), (b.2) and (b.3) for all values of time $t$. A very simple form for the matrix $A$ is obtained with the so-called restricted mixing, where $p(i,j) = 1$ if and only if $i = j$. Beside this unrealistic case in which all contacts are restricted to within a class, the proportional (or random) mixing can be modeled assuming that, for all $i, j$ combinations, the fraction of contacts of class $i$ with class $j$ is equal to the fraction of contact due to the class $j$ with respect to the number of contacts due to all classes. Then, a linear combination of restricted and proportional mixing refers to the preferred mixing.

A final option is complex choice mixing, for which an example of the associated partner choice network is given in the figure below.

![Partner choice network with 17 male homosexuals distributed in 3 sexual activity classes based on the number of partners per year](image)

In Fig. 6, a community of 17 male homosexuals is stratified in 3 classes by sexual activity. The classes contain 10, 5 and 2 individuals with 1, 2, and 3 partners per year respectively. The network generates the choice probability matrix $P$ that satisfies (b.1), (b.2) and (b.3).

$$p(i,j) = \begin{pmatrix} 0.4 & 0.4 & 0.2 \\ 0.4 & 0.4 & 0.2 \\ 0.33 & 0.33 & 0.33 \end{pmatrix}$$

This theoretical result on sexual mixing networks highlights the important roles of network structure and core groups in the dynamics and persistence of STDs. However, approximations are
still far from real mixing among individuals and related studies often refer to relatively small-scale communities.

Computer-generated networks have been developed through the years to deal with epidemic transmissions, and mathematical theory underlying such studies refers to the Complex Network Theory. After a brief introduction of relevant network proprieties in the context of infectious diseases, the most common families of networks studied are discussed below.

As mentioned, a graph (or network) is defined by nodes, namely individuals or classes of individuals, and edges between nodes, which are ‘contacts’ in epidemiological terms. Network epidemic models refer then to the set of contacts of an individual as his ‘neighborhood’, and the size of such neighborhood is the individual’s ‘degree’ $k$ (i.e. number of edges that a node has). The ‘degree distribution’ is defined as a set of probabilities $P(k)$ that a node chosen at random will have degree $k$. $P(k)$ is important for characterizing networks because it captures heterogeneity in individuals’ potential to become infected and cause further infections. In this way, the degree distribution strongly influences the recovery of epidemic threshold, totally breaking down the classical result of Kermack and McKendrick [5] in particular cases.

Further characterizations can be obtained calculating the $n$th moment of $P(k)$ as follows:

$$\langle k^n \rangle = \sum_k k^n P(k)$$

with the first moment being the average degree, the second allowing to calculate the variance, and so on.

Finally, $P(k)$ provides useful information on uncorrelated network, although real networks are often correlated with respect to the degree. This means that usually the probability of finding a node with degree $k$ depends on degree $k'$ of its neighbors and is given by the conditional probability $P(k|k')$. (See, e.g., Danon et al. [28] for further details on measurements of degree correlations).

In a network, the distance between two nodes $i$ and $j$, $d_{ij}$, is defined by the path requiring the smallest number of steps to reach $j$ from $i$. Given the number $N$ of nodes in the network, the average distance between all pairs of nodes can be measured as:

$$\langle d \rangle = \frac{1}{N(N+1)} \sum_{i \neq j} d_{ij}.$$
Analyzing epidemic networks in terms of number of steps needed to reach any node from any other shows clear implications for disease spread and control. The shorter number of steps, the quicker infection spreads.

While distances between nodes give information about the global network, there are local characterizations of epidemic networks. One of them is the centrality of a node, which influences rapidity of epidemics’ diffusion in the neighbors of such node and it also depends on the notion of shortest distance. The betweenness centrality is the most relevant measure to quantify how central a given node $i$ is in the network, and it is defined as:

$$B_i = \frac{\text{# shortest paths through } i}{N(N - 1)}.$$

Hence, the betweenness can be simply defined as the proportion of shortest paths that pass through a single node. Another aspect of the network structure at individual level is the clustering coefficient $\phi$, which measures the local density of a graph. In epidemiological terms, it represents the probability that two individuals that are neighbors of a node are also neighbors of each other. In formulas,

$$\phi = \frac{3 \times \text{# triangles in the network}}{\text{# of connected triples}}.$$

A connected triple is formed by a node that has edges with a pair of others, and so $\phi$ measures the fraction of triples that are also part of triangles. The factor of 3 guarantees that $0 \leq \phi \leq 1$. For each node $i$, the clustering coefficient refers only to the immediate neighbors of $i$ as follows:

$$\phi_i = \frac{\text{# triangles centered on } i}{\text{# triples centered on } i}.$$

In clustered network, rapid local depletion of susceptible individuals does influence the spread dynamics. While central and clustered nodes are targets for intervention strategies at individual level, thinking a network as collection of subgraphs provides an understanding of network structures at an intermediate scale. For instance, a clique is a fully connected subgraph with the simplest example being a triangle. Shifting the idea on epidemics, relevant subgraphs are those that have high density of edges between its nodes but lower density of edges with other subgraphs of the network. This is the intuitive notion of ‘communities’ within an host population that has been formalized by Newman and Givran [37] in terms of modularity measure. Modularity compares the expected number of edges within communities to the actual number of edges within communities. (See more details and further references in [28]).
Few studies focus on the impact of communities in transmission processes so far, however it seems to have a profound impact on epidemic dynamics. Computer science literature explores the conductance as valuable measure to explore a wide range of networks [38].

Following the seminal review work conducted by Keeling and Eames [26], five distinct types of networks are introduced and illustrated (Fig. 7(a)-(e)). In every figure, a network type containing 100 individuals is represented on the left. The right side of each figure shows a graph plotting infectives’ percentage over time for standard SIR epidemics solved on the correspondent network type. Considering a population of 10000 individuals with an average number of contacts per individual that is approximately four for all five networks, 100 epidemic curves (in grey) are shown together with the average curve (in black) for all major epidemics. Note that this variability within graphs is due to the stochastic nature of transmission and not variation in the network.

**Lattice network.** In lattices individual are positioned on a regular grid (usually 2-dimensional) and then contacts are localized in space. Such networks are homogeneous at individual level and highly clustered because of the localized nature of connections. As the neighbor of each node is reduced to the adjacent nodes, only short-range interactions are inducted. As a consequence lattices cannot fully capture the role of in-homogeneities.

The lattice based SIR models have a different threshold with respect to the Kermack and McKendrick [5] result. Epidemics can just remain localized around the initial focus or turn into a pandemic. The best-known examples that have analogous behavior of epidemics propagation on lattices are the forest fire models; both show an initially slow development that involves a growing of the cluster, with a wave-like progression as can be seen in Fig.7(a).

![Fig.7(a) Lattice network [26].](image)

**Small-World network.** Small-world is a concept introduced in 1967 by Milgram [39] to describe topological characteristics of social relationships and communities. Some decades ago, Watts and Strogatz [40] developed a model for constructing networks that mimic features of such social architecture by randomly adding long connections to a lattice. The degree of disorder is defined by a rewiring parameter that ranges from 0 to 1, with the extreme cases corresponding to lattice
and random network respectively (the latter will be introduced later on). Kuperman [29] states that in his previous work it has been studied the dramatic change in behavior of epidemics due to changes in the social topology. As the rewiring parameter increases, the system transits from an endemic state, with a low level of infection, to periodic oscillations in the number of infectives, showing underlying phenomena of synchronization.

The graph in Fig. 7(b) (right) depicts wave-like curves for SIR epidemics on a small-world network formed from a 2-dimensional lattice (not a one-dimensional circle – Fig. 7(b) left - for reasons of consistency) with 10 additional random long-range contacts. Hence, the transmission remains still localized due to the high level of cluster, but even few long-distance links can significantly alter the population-level spread of infection. This effect is shown by the dashed lines that plot the mean epidemic curves for an increasing number of long-range contacts to 20 and 100.

**Fig. 7(b)** Small-world network [26].

**Random network.** Random networks represent the other extreme of the rigid lattice structures, showing lack of clustering and short path lengths (while lattices have long path length due to the high clustering). In a random network, connections are randomly distributed and the spatial position of individual is irrelevant. The iconic Erdős-Rényi (ER) random graphs are built from a set of nodes that are connected at random with probability $p$ which is independent from any other contact. The degree distribution is binomial, i.e. $P(k) \approx e^{-k}$, and when the number of nodes is large it can be approximated by a Poisson distribution. Newman [25] has shown a different approach using a generating function method that allows to construct random networks with arbitrary $P(k)$.

Furthermore, Newman proves that a family of SIR models can be solved exactly on such random networks. The results include the particular case of scale-free network that will be discussed later, as according to our interest it refers to the Internet network topology studied by Pastor-Satorras and Vespignani [41].

In Fig. 7(c) (right), the disease dynamics show a clear peak of epidemic at an early stage with high number of infectives. However, it can be found that early growth rate and final epidemic size are reduced when compared with random mixing models.
Scale-free network. In most real networks there are individuals who are highly connected while others are almost isolated. Scale-free networks provide a means to achieve such extreme levels of heterogeneity. According to the Barabási-Albert (BA) model algorithm, a scale-free network can be formed starting from a core of nodes and dynamically adding new individuals (one node at each step) with a connection mechanism that replicates the choice rules of social contacts. A common characteristic of such networks is the scale-free degree distribution that follows a power law of the form \( P(k) \approx k^{-3} \).

The high level of heterogeneity characterizing such network type can be observed in Fig. 7(d) below. This scale-free network (left) presents the 74% of individuals as part of a giant component, while the remaining nodes are not interconnected. Although the average number of contacts per node is approximately 4, there is one node with 85 contacts. In epidemiological terms, such highly connected individuals play the crucial role of ‘super-spreader’ (note that they are represented by grey dots in the figure) on which depend the most relevant dynamics of diffusion. One of the most surprising results is that epidemics show no epidemic threshold when solved in scale-free networks. Pastor-Satorra and Vespignani [41] have demonstrated that the disease always propagate independently of \( R_0 \). Their new epidemiological framework is widely used to rationalize data of computer viruses and helps to understand dynamics of other communication and social network phenomena.
Comparisons between the degree distributions of the last two networks can be seen in Fig. 8 below. The figure also illustrates that the topology of ER random network (on left) has a clear peak and is close to homogeneous, while the BA scale-free network (on right) is dominated by highly connected nodes (namely ‘hubs’).

Spatial network. As the name suggests, spatial networks are generated using the spatial location of all individuals of the population. Therefore, lattice and small world networks are particular forms of spatial networks. On the contrary, random and scale-free networks do not account for spatial position. Starting from a set of locations, individuals are then connected with a probability given by a connection kernel that usually decays with the distance. Spatial networks generally have an approximately Poisson degree distribution, with a reasonably high degree of heterogeneity. In this regard, the network on the left of Fig. 7(e) has 88% of interconnected individuals that can potentially become infected, while the others are isolated.
These spatial networks have many features expected from disease networks, but it is unclear if such simple formulations can be truly representative [29]. However, they offer some mathematical insights to the wider field of spatial epidemiology. Such attracting discipline seems to date back to 1930s, when the parasitologist Pavlovsky used the concept of ‘landscape epidemiology’ to gather three simple observations: diseases are geographically limited, spatial variation lies on physical and biological changes of condition, and these conditions can be mapped to predict disease risk and incidence.

A review of the major approaches used for mapping spatiotemporal dynamics was conducted by Ostfeld et al. [35]. The authors describe new existing methods, which are spatially implicit and explicit, within the field of what they called a re-emerging discipline, that is spatial epidemiology. Furthermore, they show a promising bridge between ecology and epidemiology by discussing impacts of landscape structure on epidemiological processes, which seem to have been often neglected so far.

In recent years, a class of models has attracted many researchers in social networks: the exponential random graphs. Models based on such graphs provide a method of constructing networks with a given set of proprieties. The simple underlying propriety is that the probability of connection between two nodes is independent of the connection between any other pair of distinct nodes. Generating then a range of plausible networks using Markov Chain Monte Carlo techniques, information can be collected on network structures even if the complete network is unknown. More details are provided by Frank and Strauss [42].

As it can be seen, the majority of the studies on disease transmissions on networks focuses on static networks where all edges remain unchanged over time and have equal weight. In reality, frequency intensity and duration of contacts are all time-varying. These dynamic networks strongly influence real epidemics when looking at long-term impacts. Nevertheless, how to capture the structure of such dynamic networks is a substantial challenge of epidemiological modeling.
In this regard, *co-evolutionary or adaptive networks* take into account dynamics of the social links. The behavior of models based on adaptive network is determined by the interplay of two different dynamics that sometimes have competitive effects. These are the disease propagation and several protective countermeasures against such spread. For example, consider the case in which susceptible individuals of a host population, after learning about the existence of infectious individuals, try to avoid them. Another case is when the health policies promote the isolation of infectious individuals [43].

Under two opposite dynamics arising from epidemics and social reactions to epidemics, the adaptive network shows a new phenomenon of bistability. Risau-Gusmán and Zanette [44] show that breaking links between susceptible and infective individuals, and connecting then each susceptible to a new neighbor randomly chosen, make possible to completely eliminate the disease. This coincides with reality, as contact switching is proved being an effective control strategy in epidemic outbreaks.

In general, current research in epidemiology is moving from analytical methods to computer simulation techniques and other tools to track such complex dynamics of changes into epidemic models. Creating synergies between biology and computer science is the aim of Computational Epidemiology.

**Computational epidemiology**

Many epidemiology studies benefit of multidisciplinary approaches for making advances and developing a proper understanding of the dynamics of epidemics. Motivated by the fact that the method of trials is prohibitively expensive and unethical in the context of epidemiology, computer scientists have provided valuable tools to capture complex dynamics of diseases’ spread. The research domain accounting for this synergetic collaboration is named Computational Epidemiology. Cornerstones on the use of IT tools in the practices of epidemiology are really well presented in [45].

The growing recognition that multi level factors and interrelations among these factors are often characterized by dynamic feedback and changes over time, resulted in calls for new technologies and simulation tools potentially able to capture such dynamic complexity into models. In the context of epidemiology, arguments for this method shift to complex dynamic systems can be found in [46].
Fig. 9 captures the complexity of epidemiological issues, including all the factors of influence that lead to the real transmission dynamics of diseases.

![Fig.9 The complex ecology of epidemics [47].](image)

Swarup et al. [47] describe that individual, social, logistical, and structural factors affect epidemic outbreaks beyond physical aspects of the disease such as transmission modes, incubation periods, infectious periods, etc. Many of these factors listed in Fig.9 are interrelated, and it often turns in the inadequacy of traditional analytical methods in addressing such complexities. As a consequence, the emerging use of computational approaches is a current challenge of epidemiology modeling. Mainly, epidemiologists are looking for tools with the ability to capture the complexity of human interactions and behavior. A review of studies focusing on how to model the influence of human behavior on the spread of infectious diseases was conducted by Funk et al. [48].

Overall, the major modeling paradigms in systems science methods are System Dynamics, Network Analysis and Agent-based Modeling. Luke and Stamatakis [6] present three case studies where these methods have been used in the areas of epidemiology, emphasizing the utility of systems science in Public Health.

Network Analysis is a research method that lays the foundations in a number of different disciplines, for which mathematical insights have been presented in the previous section. With the development of specialized network analysis software, the new science of networks is being used in almost every area of science [6]. However, epidemiologists and other experts on the field that are not trained to understand mathematical theories and complexities of certain computer programs. This is the reason for the development of user-friendly tools [49]. System Dynamics and Agent Based modeling support the increasing demand for such tools.

System Dynamics (SD) is a methodology centered on the fact that the complex behaviors of systems (organizational, social, etc.) are the result of ongoing accumulations (of people, information, money, etc.) that change according to interaction of variables within complex
feedback structures. In particular, SD involves development of causal diagrams and computer simulation models that are used for what-if scenario evaluations to predict epidemics’ spread and decision-making in the context of Public Health. The seminal book of Sterman [50] presents the classical SIR model developed using System Dynamics. Further references on background and opportunities of SD modeling for Public Health can be found in [51].

While System Dynamics offers a continuous and time-dependent domain of variables that accounts for the global system behavior driven by a set of differential equations underlying the model, Agent Based Modeling models the real world as a set of behaviors of agents. Agent-Based method can be defined as a decentralized and interaction-oriented modeling paradigm in which the overall dynamics of infection is the result of a variety of events that involve the single agents. Patlolla et al. [49] conducted a survey of the state-of-the-art in Agent Based modeling that empathizes its unique features for coping with the emerging area of computational Epidemiology. Also, comparisons of SD and AB simulation models applied to epidemics can be found in [52].

A fourth computational approach refers to the so-called synthetic information methods. Synthetic information methods are sophisticated agent based models able to provide very realistic approximations by combining multiple data sources that cannot be gathered through surveys or other methods. In this regard, Madhav et al. [53] developed the Synthetic Information Environments (SIEs) approach, that consist of four components: a statistical model of the host population (i.e. synthetic population), an activity based model of the social-contact network, disease-progression models, and models for evaluating interventions and individual behavioral adaptions.

In line with Swarup et al. [47], this section identifies Computational Epidemiology as a challenge domain for multi-agent systems. In this direction, it can be easily drawn the parallel with the virtual world discussed in the next section. Complex cyber dynamics are regulated by actions of many agents involved in the so-called systems of systems. The related studies refer to critical infrastructures interdependences and protection: emerging field where high-performance computing paradigms strongly contribute to the work of today’s researchers in addressing security challenges of cyber-physical systems.

**From epidemiology to cyber epidemics modeling**

Biological systems are dynamic, evolving, self-organized, highly complex, and continuously adapting to an ever-changing environment. Such features attracted many researchers, which
attempt to understand complicated phenomena of totally different natures by lessons learned from biological behaviors. In particular, when dynamics and complexity of systems are exponentially growing such as in crisis situations, parallels and analogies with biological concepts are extremely helpful in understanding uncertain and interdependent feedback structures. This is the case of epidemics: research efforts in modeling transmission of malaria, AIDS and many other infectious diseases have been inspiring and highly contributing to understand newer, but not less dangerous, crises such as cyber epidemics and related computer security problems.

Previous sections illustrate how epidemiological patterns have been developed to model complicated dynamics of infectious diseases. The abstraction from details of biological pathogens makes it possible to apply these models into disparate fields. See, e.g., the close collaboration between sociologists and epidemiologists in the context of Social Network Analysis [54].

In cyber terms, of particular interest is the comprehensive taxonomy on biological concepts successfully applied to computer networking made by Meisel et al. [55]. This section aims to explore how the well-established field of epidemiology provided solid pillars for research towards the relatively new branch of cyber crisis modeling. There are several valuable insights from the metaphor of infectious diseases’ spread for “cyber epidemics”, but such metaphor has several limitations in applying epidemiological models to challenges of the digital world.

Referring to the categories used by US National Research Council for classifying research programs in life sciences, the survey of Meisel et al. [55] is organized by respective areas of application in computer network research as follows in Fig. 10.

![Taxonomy of computer network research inspired by biology, organized by the area of application [55].](image)

According to the taxonomy in Fig.10, many authors recognized relevant applications of the so-called “epidemic algorithms” to the spread of desirable information through wireless and mobile
ad-hoc networks (e.g. epidemic routing for MANETs [56]). Other research works used self-organized “cyberentities” with biologically inspired properties to build distributed systems. An example is the pioneering work by Wang and Suda [57]. They describe the Internet architecture as a set of interconnected nodes (i.e. cyber entities) with different capabilities to provide a service to the users, and characterized by bio-life cycles of reproduction, dead, and mitigation across the network topology.

As this literature review explores the security application domain and related cyber crisis situations, this section focuses on what Meisel et al. [55] identify as the strongest of all the biological connections: the application of epidemiology to malware propagation and intrusion detection in computer networks. Drawing parallels between epidemics and computer viruses spread is not a new idea [58]. It was in 1993 when a special report of IBM experts [59] deeply described first efforts in constructing a theory for computer security based on epidemiological language.

Two of the IBM researchers, namely Kephart and White [60], were the first to apply the epidemic SIS model to the spread of computer viruses. They propose a directed-graph model in which a susceptible node becomes infected only if there is a connecting edge from an infected node to the susceptible one. As illustrated in Fig. 11 below, each edge has different probability of transmitting infection, $\beta$, and cure rate, $\delta$. With their model, Kephart and White demonstrate the strong impact of the network topology on how a virus spreads (Fig. 11 right).

![Fig.11 SIS model on directed graph and comparison of infected (i) over time for different network topologies [60].](image)

Almost 15 years after the pioneering work of Kephart and White, Pastor-Satorras and Vespignani [41] argue that the view obtained until then with the widely used SIS modeling of computer virus epidemics was ‘very instructive but not completely adequate to represent the real phenomena’. Analyzing real data of computer viruses infections, they model the Internet topology with the particular class of scale-free networks. Their study led to a very surprising result: the absence of an epidemic threshold and associated critical behavior on scale-free networks. This new epidemiological framework changes many conclusions of the traditional threshold theory by
McKendrick-Kermack, and it has been helpful to understand particular diffusion phenomena of social, biological and communication systems.

Over the years, many sophisticated computer viruses came together with the rapid growth of the Internet. The consequent growing complexity of network structure dynamics attracted many researchers towards the emerging field of computer security. The majority borrows epidemiological approaches and somehow adapts them to “cyberepidemics” modeling with ‘little modification and much success’ [55].

Opposite to the Kephart-White SIS model, in 2002 Zou et al. [61] adopt the SIR epidemic model to analyze the Code Red worm propagation. A most recent research considers the SAIR model [62], a modified version of the SIR epidemic model that includes antidotal population compartment, A, to study the operational state of the network and its recovery times when a perturbation appears. Also, the literature evidences interesting studies on a stochastic SLBS model and its generalizations [63]. This model considers the infected computers within two classes based on different probabilities to get treatment: breaking-out computers, B, and latent computers, L. The effect of quarantine, Q, on recovered nodes, R, is analyzed using the modified SEIQRS model [64].

All above works provide valuable theoretical insights, but they are far from being applied in real contests. However, some experiments on real and synthetic networks are being done to demonstrate the accuracy of a new analytic model for virus spread on arbitrary graphs [65]. This study proposes the epidemic threshold as function of a single parameter capturing the virus propagation proprieties: the eigenvalue.

Apart of analogies and few extensions of classical SIS and SIR epidemic models that allow to get a first understanding of diffusion processes, it seems there is a stream of literature on computer viruses that focuses on detection and prevention rather than modeling their spread [55]. As depicted in Fig.10, a branch of biological inspired research applied to cybersecurity refers to artificial immune systems. Here, biological analogies clearly lie on the fact that protecting computer networks is a new problem for which biology already has a solution: the immune system. First research efforts in “computer immunology” have been done by Forrest et al. [66]. The figure below gives an impression on how insights from natural immune systems have been helpful in understanding computer security problems.
Fig. 12 depicts three standard phases of attack and recovery mechanisms occurring within biological, but also cyber, systems. Once the infection (red) affects the system (blue), it has to be recognized and then destroyed by immune system detectors (green). In computer systems, the process is clearly analogous: IT-administrators need first to prevent intrusions, and countermeasures are needed to identify, mitigate, and combat attacks in case unknown malwares exploit network vulnerabilities. This sounds like the description of an ideal Intrusion Detection System (IDS), therefore many computer scientists have attempted to use artificial immune system approaches in this context. One of the earliest designs, comprehensive of actual implementation in the IBM’s virus lab, refers to Kephart [67].

Going back to epidemiological patterns, immunization strategies have been largely investigated by governments to eradicate several epidemics affecting populations through the years. Using the SIR model, Madar et al. [68] analyze the effects of random, acquaintance and targeted vaccinations on epidemic dynamics in complex networks, in particular, scale-free networks. Not surprisingly, these “vaccination methods” have been explored to develop new security policies for eradicating computer viruses in networks (e.g. [69]). Different immunization schemes on scale-free networks with nonlinear infectivity were studied in [70]. A mathematical review of major results in this context can be found in [71].

Wang et al. [72] argue that immunization is well-understood as approach to defending against viral infections in the classical epidemiology sense. In the computational realm, however, it has not been examined closely. Emphasizing limitations of analytical approaches, they proposed a simulation study effects of random and selective immunities on different network topologies.
Discussion

Overall, this article provides a reference guide that may facilitate rational decisions in choosing models for applications. Several mathematical insights to understand disease spread are highlighted, and core building blocks of models and research patterns in epidemiology are identified. Many approaches that range from traditional deterministic and stochastic models to network analysis and computer simulations have been introduced in the context of epidemiology modeling.

According with our particular interest in cyber crisis modeling, we conclude that mathematical insights from epidemic modeling allowed cybersecurity research to quickly move one step ahead. Despite obvious connections handed down from epidemiology, recent works on cyber attack and defense modeling do not focus on epidemic models and rarely mention their epidemiological roots. Rather, computer security committees continuously claim the lack of proper and comprehensive methods to understand IT-security problems, operational disruption dynamics over time, their impacts on business models and viceversa. Beyond the solid research pillars provided by biological epidemics modeling, a lot of work needs to be done to understand dynamics of complex cyber crises daily affecting enterprises’ business.

In general, the new persistent threat of network security has a lot in common with problems that epidemiology has encountered and resolved. Over the years, approaches and techniques from epidemics modeling have been adopted and applied to understand diffusion dynamics and effects of recovery strategies in cyber crisis situations. Mainly, epidemiological models reveal conditions under which viruses spread and enable qualitative analysis of complex relationships between variables over time [73]. But it was only in 1998 when a major expert of the IBM research group, namely White, announced that despite the study of biological epidemiology had been extended to cyber domains, there were still open problems and the evolving technology would have generated plenty of new problems to be solved in the field of computer security [74]. Actually the times of the fast spreading viruses seem to be over. There is an infrastructure to distribute “medication” or “immunization” effectively and there is an understanding of how to build robust networks. Modern “effective” cyberthreats include highly targeted but slowly spreading malware as, e.g., Stuxnet [75] or targeted attacks as ransomware [76]. It is clear that increasing mysteries around cyber crises would have been calling for new techniques and methods able to capture dynamics of todays’ cyber conflicts such as zero-day exploits [77], as well as to assess costs related to the rapidly evolving cyber crime [78]. What remains is however the challenge to model the dynamics of cybercrises and the heterogeneity of computer networks and the impact of heterogeneity on the spread of malware.
Nowadays complex systems such as the Internet are only optimized to be robust against expected failures, but the main threat is represented by unknown attacks that could cause cascade failures breaking down critical infrastructures [79]. Therefore, computer networks need to account for high resiliency in regards to unexpected failures. As companies are expecting more and more cyber incidents with higher and higher costs each year [73], there is a strong need of proper decision-making supports for more effective IT investments’ strategies and more resilient infrastructures.

A next part of the state of the art analysis will deal with methods to analyze dynamics of (Cyber) crisis situations that deal with attacker models and heterogeneous systems. In this context, the use of Game Theory seems to be a promising approach that we aim to explore.

References


A Brief Introduction to the Emergency Service Sector

Megan L Anderson

Introduction

The emergency services are among the many components of modern society that tend to be taken for granted. Indeed, hypnotic rotating lights and ear-splitting sirens have become characteristic sights and sounds of the contemporary city-scape. Yet, the emergency services have, of course, not always existed as such. Even today, countries vary drastically in terms of the sophistication and organization of their emergency service sectors, in addition to the services actually provided. As a result of the 2008 financial crisis and seemingly universal cuts in public expenditure, the emergency services are among the many public services that have been forced to do more with less. This has led to some novel inter and intra organizational changes at the field level, whereby the separate organizations are turning more to their collective identity so as to provide more efficient and effective services for citizens.

The (re)organization of the emergency services sector has been increasingly featured in newspaper headlines around the world. Relatively recent articles in The Guardian (Meikle 2013), New York Times (Davey 2011), Boston Globe (Neyfakh 2013), and ABC (Hill & Gibson 2014) feature the contentious issues of public safety consolidation, emergency service mergers and restructuring in localities from the lakes of Michigan to the shores of South Australia. As of September 2011 more than 150 agencies across the United States have been identified as having some form of public safety consolidation (Wilson & Grammich 2012, p.5). And in the UK, Sir Ken Knight (2013), the former chief fire and rescue adviser, released a report in which he recommended mergers and restructuring as vital future steps for emergency service organizations across the UK.

Greater collaboration, joint-working, and organizational consolidation are not just about cutting costs. It makes sense that organizations with such great task overlap work together more closely to streamline operations, communication, knowledge and resource sharing. Further, the logic for collaboration is evermore reinforced as incidents become more complex, with the increased exposure of societies to a more interconnected urban risk landscape. Despite the importance and practicality of considering the emergency service sector in its entirety, much of the relevant research in this domain still focuses on each service in isolation. Thus, the objective of this chapter is to provide an overview of the sector as a whole. Section 1 provides a brief history of
the origins of organized and professional emergency service provision, with particular attention to London. Section 2 provides an overview of the contemporary organization of emergency services, and identifies three common organizational models. Section 3 outlines common ways in which the emergency services are working together to provide more efficient and effective service delivery. Finally, Section 4 concludes with a summary and a discussion of the future of the sector.

A Brief History of the Emergency Services

The emergency services as we know them today are a product of industrialization and urbanization. The booming cities of the industrial revolution led to a proliferation of dangerous workplaces and living spaces and a greater concentration and interconnectedness of risks. With the industrial landscape came more industrial accidents, crime, fire and disease. Incidents became frequent but citizens rarely received quick treatment, as the capabilities and infrastructure to deal with such occurrences could not keep pace with the booming demand. Death or disability from untreated injuries was common, fires destroyed entire neighborhoods, theft and rioting were commonplace and diseases plagued entire cities. Figure 1 depicts the slums of London, illustrating the poor and overcrowded conditions of the rapidly industrializing city.

Figure 1. Over London by Rail. (Doré 1872).
How did these booming urban societies organize themselves to deal with increasingly complex safety and security concerns? Firstly, they did not immediately develop the emergency services as we know them today. The development of separate services for police, fire and ambulance with an entirely separate set of social support services is a mid-twentieth century development. This brief historical overview focuses on the years shortly preceding and shortly following the establishment of these organizations in London. As many of the modern organizational forms of emergency service organizations originated in the UK and were spread around the world by way of colonial rule, focusing on historical developments in this particular context is relevant to developments in many other countries and cities. It is nevertheless important to be aware of the many other influential organizational forms that evolved elsewhere, especially in the other colonial powers. These differences will be touched upon in Section 2. Moreover, while the term “Emergency Services” most commonly refers to three functions, performed by three separate organizations (Police Department, Fire Department and Ambulance Service) in a given area, it is important to note that there are also many countries and cities where fire, rescue and ambulance functions are all performed by a single organization. Again, these differences in organizational form are further elaborated upon in Section 2. Finally, many countries and cities have additional emergency service organizations for specialized functions (e.g. coastguard, mountain rescue, HAZMAT etc.). This chapter focuses specifically on the three most common organizations.

**The Police Service**

The origin of the modern police services is commonly traced back to 1829 London, with the establishment of the Metropolitan Police Service (MPS) (e.g. Fogelson 1977). Prior to this, policing activities in London and the rest of the UK were disjointed and unprofessional (Lyman 1964, 141). Early 19th century London was policed by 450 constables and 4,500 night watchmen (The National Archives), while the Thames River Police patrolled the busy waterways, and the Bow Street Runners apprehended criminals on behalf of the Bow Street Magistrates Court (UK Parliament 2015).

Meanwhile, across the channel, other European nations had established more organized and professional forms of policing. The system in Paris was perhaps the most notable, with the best-organized, paid police force (Garrioch 2012: 35). However, as Britain was at war with France from 1793 to 1815, many in the UK were weary of anything French on principle (The National Archives) and the Paris police system was considered by many as symptomatic of absolute monarchy (Garrioch 2012: 35). Despite opposition to a more organized policing system, the expansion of London and other industrial cities during the late 18th and 19th centuries put the maintenance of law and order high on the public agenda. Statistics from this time revealed that crime was increasing at an alarming rate, peaking especially during the depression years of 1815-1817.
Moreover, Twelve of London’s parishes, with a total population of twenty thousand, had no night police and by 1828 one person in every three hundred and eighty-three was a criminal (Lyman 1964: 149). As a result, in 1812, 1818 and 1822, Parliamentary committees were tasked with investigating the subject of crime and policing1. The investigations revealed the severe shortcomings of the current policing system, but failed to result in a necessary, and revolutionary solution. Finally the 1828 Committee, led by Home Secretary Sir Robert Peel, outlined a novel plan to establish a centralized and unified system of police under the Home Secretary, with responsibility for the whole metropolitan area. Peel believed that the function of a new and improved police service should focus primarily on crime prevention—that is, preventing crime from occurring instead of detecting it after it had occurred. To do this, the police would have to work in a coordinated and centralized manner, provide coverage across large designated beat areas, and also be available to the public both night and day. The following year Peel introduced "A Bill for Improving the Police in and Near the Metropolis” in order "to substitute a new and more efficient system of Police in lieu of such establishments of nightly Watch and nightly Police.” The area in charge of the Police Office was to be called the Metropolitan Police District, and included all of Westminster, and parts of Middlesex, Surrey, and Kent. The Bill also contained rules for the duties, powers, and discipline of the paid constables (Lyman 1964: 150). On 29 September, 1829, the Metropolitan Police Act2 was passed, enabling the establishment of the new service.

Within the next year seventeen police divisions were established. Each division was in the charge of a superintendent, under whom were four inspectors and sixteen sergeants. The regulations demanded that recruits should be between 20 and 35 years old, well built, at least five feet seven in height, literate and of good character (Archbold 2013, 4). To quell public concern regarding the powers of the new police service and increase its legitimacy, Peel identified several principles to which all recruits were to be held accountable (Archbold 2013, 4). Command, discipline and accountability would be ensured through a military-like organizational structure and a central headquarters would provide a physical place for the public to interact with the new organization. Police officers would wear appropriate uniforms and badge numbers so as to be easily identified by the public. They were not to carry firearms and receive appropriate training to effectively carry out their work (Archbold 2013, 4).

---

1 See http://www.britishparliamentarypapers.com/acatalog/Police.html for reports from the Select Committee on the Police of the Metropolis

2 See http://www.legislation.gov.uk/ukpga/Geo4/10/44
Over the decades to follow, more divisions were created to keep pace with the growing city. By June 1, 1830, the force consisted of three thousand, three hundred and fourteen (3,314) men, and the Metropolitan Police District covered Whitehall, Westminster, and twelve other boroughs. By the terms of the Act the City was excluded, and remains so to this day (Lyman 1964, 153). Moreover, as the service grew, it began to acquire other organizations and their established functions. For example, the Bow Street Horse Patrol was incorporated into the force in 1836 and operated in the outlying Metropolitan divisions. Similarly, the second Metropolitan Police Act 1839 converted the River Thames force into the Thames Division, absorbed the Bow Street Foot Patrol and extended the Metropolitan Police District to a fifteen mile radius.

Into the 20th century, Peel’s police force provided the underpinnings for the contemporary policing business model. By the 20th century, policing in many towns and cities in both the UK and around the world started to resemble the MPS. Technology further influenced the way police operations evolved. Telegraphy, the automobile and the two-way radio were some of the most influential technological innovations that impacted upon police work throughout this century. Along with technological advancements, the size of police departments grew to match the

---

3 See [http://discovery.nationalarchives.gov.uk/results/r/? q=MEPO%2015](http://discovery.nationalarchives.gov.uk/results/r/? q=MEPO%2015) for maps of the districts and their changing boundaries.
demand of growing urban populations. This organizational growth meant further organizational specialization and complexity. Departments developed special units and bureaus for specific problems and niche services.

The force continued to be controlled directly by the Home Secretary until 2000, when the newly created Greater London Authority was given responsibility to oversee the force, through the Metropolitan Police Authority. The MPAs ceased to exist on 16 January 2012, when its functions were transferred to the Mayor's Office for Policing and Crime (MOPAC). The MPS currently operates across an area of 620 square miles, serving a population of approximately 7.2 million (Mayor’s Office for Policing and Crime 2015).

**Fire Service**

Firefighting responsibilities prior to the 18th century were typically in the hands of local communities and night watchmen, who used very basic and inefficient firefighting tools and techniques. With many homes made of wood and thatch, and the use of open flames for cooking and lighting, major fires were a common part of life. Firefighting services became more organized after the Great Fire of London in 1666, which destroyed 13,200 houses, 87 parish churches, The Royal Exchange, Guildhall and St. Paul’s Cathedral (London Fire Brigade 2015). As a result, thousands were made homeless, and many died from disease and exposure to the cold during the time of reconstruction. Debtors’ prisons overflowed with numerous businesses and citizens who had become financially ruined (London Fire Brigade 2015).

In response to the social devastation, a new, more organized system of firefighting was implemented, whereby people paid a fee to newly established fire insurance companies to insure their properties against damage. Each fire insurance company maintained its own fire engines and fire brigade, tasked with suppressing fires in buildings insured by its company. They marked their respective insured properties with metal plaques of the company emblem, called ‘fire insurance plaques’ (London Fire Brigade 2015). The first such insurance company, called Phoenix, was established by Nicolas Barbon in 1680. Many more soon followed, including the Friendly Society (1683), Hand-in-Hand (1696) Sun Fire Office (1710) and Royal Exchange Assurance (1720) (see Robert 1910). The insurance company firemen had minimal training and distinguished themselves from rival brigades with brightly colored uniforms (London Fire Brigade 2015).
Eventually, as demands grew on this disjointed firefighting system, the respective companies began to cooperate. In 1833, 10 insurance company fire brigades were consolidated into the London Fire Engine Establishment (LFEE) to provide the public with a more efficient and effective firefighting services. In other cities around the UK, insurance fire companies had already been consolidated. Some cities, like Edinburgh (1824), already had a fully consolidated, publically funded fire service (Wallington 2005: 19). James Braidwood, the Firemaster of Edinburgh’s department was thus the obvious choice to lead the newly established LFEE and he would remain its Chief Officer for 28 years. At the time of its establishment, Braidwood’s department had 80 firemen at 19 strategically placed fire departments across London (Wallington 2005: 22). By 1853 this number grew to 110 firemen, equipped with 25 horse drawn manual pumps and 28 hand-propelled manual pumps (Wallington 2005: 26). Braidwood was tragically killed in the devastating Tooley Street fire in 1861. He was soon replaced by Captain Eyre Massey Shaw that same year, who was to become even more famous a Chief Officer than Braidwood and an international advocate for fire prevention and greater fire safety throughout the civilized world (Wallington 2005: 31).

As a result of the Tooley Street fire and other large and costly conflagrations, insurance premiums skyrocketed to the dismay of businesses and the general public. This, in turn, spurred protestors to lobby the government to fund and manage the fire brigade at public expense. In 1862, with mounting pressure, a select committee was charged with investigating and recommending improvements to London’s fire service. Much debate ensued, and there was even consideration of a combined fire and police service for London (Wallington 2005: 34). Finally, in 1865 the Metropolitan Fire Brigade Act⁴ was passed, which placed the responsibility for the organization and funding for London’s fire brigade under the Metropolitan Board of Works. From here on,

---
Massey Shaw was able to expand the brigade to around 43 stations and 232 firemen across four districts (Wallington 2005: 35).

Figure 4. Caricature of Eyre Massey Shaw (1830-1908). Caption read "He well deserves his popularity" (Vanity Fair 1871)

Into the 20th century, technology would play a significant role in the evolution of the brigade (renamed London Fire Brigade (LFB) in 1904). Innovations, particularly in transportation and firefighting equipment, led to a more efficient and effective service. The war years and growth of London also influenced the organizational structure of the service. During the Second World War, fire services were amalgamated into a single National Fire Service. In 1948, responsibility for fire services was returned back to local authorities. With the formation of Greater London in 1965, the LFB absorbed the fire services in the surrounding boroughs. In 1986 the LFB came under the control of the London Fire and Civil Defense Authority, before being replaced by the London Fire and Emergency Planning Authority (LFEPA) in 2000. The Greater London Authority was established that same year and given responsibility for the LFB and other municipal functions. Today, the LFB employs just under 6,000 employees and is organized across 103 stations and five divisions (London Fire Brigade 2015).

**Ambulance Service**

While the Metropolitan Police Force evolved with the criminal justice system, and the London
Fire Brigade with the insurance and local government systems, London’s ambulance service evolved with its hospital system and the establishment of the Metropolitan Asylums Board (MAB). The MAB itself was a novel public service innovation. Passed by parliament in 1867, the Metropolitan Poor Act\(^5\), aimed to establish facilities for the ‘Sick, Insane, and other Classes of the Poor, and of Dispensaries; and for the Distribution over the Metropolis of Portions of the Charge for Poor relief; and for Other Purposes relating to Poor relief in the Metropolis.’ The Bill empowered the Poor Law Board to fund and establish new hospitals and the care of patients within them.

Prior to 1881, a patchwork of unregulated urgent medical aid systems had developed alongside the hospital system. Most street accident cases during the time were removed by wheeled litters located at police stations, or attended to by the St. John Ambulance Association, with its own thirty-five voluntary first aid posts across London (Ayers 1971: 188). The ill and injured were usually transported by the police, fire brigade or taxi-drivers in wheeled stretchers, named ‘litters’ (London Ambulance Service 2015).

Finally in 1881, the Metropolitan Asylum’s Board (MAB) began designing and implementing a large network of land and water based ambulances. Six ambulance stations adjoined the MAB hospitals, so that the London administrative area was almost completely covered by a three mile radius from each station (Ayers 1971: 188). Nevertheless, these early ambulance services were intended only for the transport of patients with infectious diseases. There was still yet to be a publicly provided service for non-infectious patients, although this was considered from time to time (Ayers 1971: 189). After various failed attempts to persuade politicians of the need for such a service, the MAB established an informal arrangement with ambulances of differing colors for infectious and non-infectious patients (e.g. cases of accident and sudden illness in the street). Meanwhile, to the surprise of the MAB, Parliament passed a private member’s bill which enabled the establishment of an ambulance service for non-infectious cases within the County of London, to be under the control of the chief of the London Fire Brigade. After years of co-existing systems, the fleet of 107 MAB ambulances was taken over by the LCC in 1930, when the Government announced proposals for the reorganization of local government in England and Wales (London Ambulance Service 2015). This resulted in one public transport system for all cases of illness and accident in London.

---

\(^5\) See https://archive.org/details/metropolitanpoo00glengoog
During the Second World War, the government set up an auxiliary service to handle the surge in demand during the bombing of London by Nazi Germany. After the war, the establishment of the National Health Service through the National Health Service Act of 1948 stipulated that ambulances be available for all those who required them. When the Greater London administrative area was established in 1965, all nine ambulance services operating in the urban region were amalgamated into the London Ambulance Service (LAS). The present day LAS became an NHS Trust in 1996, after being handed over from the South West Thames Regional
Health Authority following the further reorganization of the NHS. The LAS has a staff of 4,500 located at ambulance and support offices around London. The city is divided into three operational areas (east, south, and west) with a total of 70 ambulance stations among them (London Ambulance Service 2015).

Contemporary Organizational Structures of the Emergency Service Sector

An International Overview
Contemporary organizational structures of emergency services are highly contextual, reflecting the historical, legal and political evolution of the societies in which they are embedded. More specifically, as in the case of the UK for example, each service evolved alongside wider institutions. As society came to consider that these services be provided to all, regardless of ability to pay, they became publically provided in many cities and countries. There are nevertheless many examples of privatized emergency services, especially in the case of ambulance services (Morris 2014). While most localities in the UK and abroad have emergency services that are publically provided, they exist among complex assemblages of public-private partnerships.

There are other notable differences between the structure of each respective emergency service organization across countries (i.e. differences in intra-organizational structure), which often influence the ways that they work together at the national, regional and local levels (inter-organizational structure). Some countries maintain multiple municipal police, fire and ambulance services, with slightly different arrangements for less urbanized areas. Other countries have regional departments, with a different police, fire and ambulance service for every region, state or territory (e.g. Australia, Germany). As many police, fire and ambulance services developed locally, for the purposes of serving particular cities and towns, it is still common for countries to have many separate departments for each respective locality at either the regional or municipal level. As cities have grown and merged, a trend has been to consolidate various local departments into a single, national organization. The police in The Netherlands, for example, was reorganized into one single national police force in January 2013. The new National Police of the Netherlands, under the Ministry of Security and Justice, is made up of 10 regional units, a Central Unit for specialist police activities and a Police Service Centre for all business operations.

---

6 See http://www.legislation.gov.uk/ukpga/1990/19/contents

7 See http://www.government.nl/issues/police/police-reorganisation-a-national-police-force
Scotland similarly merged all eight territorial police forces in 2013, along with its eight regional fire services resulting in the Police Service of Scotland and the Scottish Fire and Rescue Service\(^8\). Also common is a combination of nested municipal, regional and national services operating in a complex multi-level governance system.

Furthermore, unlike in the UK and many cities and regions around the world, some localities have one organization devoted to the public provision of both fire and rescue services, as well as emergency medical and ambulance care. In many cases the consolidation of these two services under one organization has happened in the last few decades. In Singapore, for example, the Singapore Fire Service (SFS) and the Singapore Civil Defense Force (SCDF) were formally integrated in 1989 due to the similarity in roles and functions. The SCDF, under the purview of the Ministry of Home Affairs, now provides fire-fighting, rescue and emergency ambulance services; mitigates hazardous materials incidents, as well as formulates, implements and enforces regulations on fire safety and civil defense shelter matters (SCDF 2015). Similarly, the New York City Emergency Medical Service (NYC*EMS) merged with the New York City Fire Department to become the New York City Fire Department Bureau of EMS in 1996 (New York City Fire Department 2014). This organizational structure is not uncommon; in fact, it is arguably becoming the norm.

An uncommon organizational development particular to the American context has been the establishment of fully consolidated emergency service departments, whereby policing, firefighting and emergency medical services are provided by fully cross-trained officers operating under a single organizational structure (typically called a public safety department). Heinonen and Wilson (2013) highlight the history of consolidated police and fire departments, with the first created in 1911 in Grosse Pointe Shores, Michigan. Consolidated departments in Oakwood, Ohio, Butner, North Carolina, Oak Park, Michigan, Beverly Hills, Michigan, and Sunnyvale, California are among those that are more than a half-century old. 140 consolidated departments of varying forms have been identified in 27 states in the U.S., with approximately half operating in the state of Michigan (Heinonen and Wilson 2013).

Overall, three basic organizational models of municipal emergency service provision can be distinguished. Model A, the tri-service model, entails the complete organizational separation of the three services (e.g. police, fire and ambulance). Model B, the bi-service model, entails two organizations: a police department, and a department responsible for fire, rescue and emergency medical care (the EMS function is commonly subsumed under the Fire Department as a bureau

---

\(^8\) See http://www.legislation.gov.uk/asp/2012/8/contents/enacted
or sub-unit). Finally, Model C, the consolidated model, refers to the complete consolidation of all three services under one organizational structure, typically in the form of a Public Safety Department. This model is the rarest, and examples of such systems are overwhelmingly located in the U.S.

**Figure 6. Organizational Models of Municipal Emergency Service Provision**

**The UK**

Emergency service provision in municipalities and other localities in the UK are typically organized in line with Model A, with a separate department for police, fire and ambulance services. This is as a result of the overall emergency service landscape in the UK, which is complex and fragmented. Emergency ambulance services are provided by National Health Service ambulance trusts, of which there are currently 10. This is in addition to the Welsh, Scottish and Northern Ireland Ambulance Services, and separate arrangements for smaller island territories. Most of these operate within the boundaries of the regions of England, the highest tier of subnational division used by Her Majesty’s government. Police forces are organized by Police Areas defined by Section 1 of the Police Act 1996, of which there are 43 excluding the Metropolitan Police District and the City of London police area, defined by Section 76 of the London Government Act 1963 and the City of London Police Act 1839 respectively. Scotland and Northern Ireland both have a single, respective police force. Finally, the fire and rescue services in the UK operate under separate legislative and administrative arrangements, resulting in over fifty separate organizations, while Scotland and Ireland have centralized FRSs.

In light of this fragmentation, the UK government has acknowledged the need to create mechanisms and frameworks for inter-organizational collaboration (Cole and Marzell 2010, 2). The Civil Contingencies Act (2004) is perhaps the main manifestation of this, establishing a
coherent framework for emergency planning and response ranging from local to national level\textsuperscript{9}. It also mandates Local Resilience Forums (LRF), which are multi-agency partnerships made up of representatives from local public services, including the emergency services, local authorities, the NHS, the Environment Agency and others, with the aim to plan and prepare for localized incidents and catastrophic emergencies. Meanwhile, however, various voices across government have been advocating more concrete forms of service collaboration in ‘routine’ emergency service provision\textsuperscript{10}.

**Collaboration and Integration in the Emergency Service Sector**

The UK government, along with various other national and local governments, has been promoting more inter-organizational collaboration in the emergency service sector. There are a variety of different and innovative ways that police, fire and ambulance services have come to work together more effectively and efficiently. These initiatives vary across localities and are motivated by a number of factors. Some initiatives leverage new information and communication technologies to streamline operations, while others entail new collaborative organizational forms. Many involve a combination of various new structures and ways of working, in terms of technology, process, service and organization. A few common initiatives include: shared incident command structures and protocols, co-location, joint-training, joint-procurement, shared back-office functions, co-response and complete organizational consolidation. These various forms are further outlined in the following sub-sections.

**Incident Command Systems and Joint Protocols**

Incident Command Systems (ICS) provide a standardized approach to the coordination and command of emergency response. Harsh wildfires in California in 1970 compelled local, state and federal agencies to streamline their response efforts through common language, management concepts and communication (Moynihan 2009: 896). They developed a system through which authority could be temporarily centralized in order to direct disparate organizations, leading to a more coordinated and efficient response effort. The system was soon adopted outside of the California wildfire context, and prepared for a number of emergency scenarios and networks of response organizations (Moynihan 2009: 896). Today, countries have developed various national and regional ICS’s of their own. The U.S. has the National Incident Management System (NIMS),

\textsuperscript{9} See http://www.legislation.gov.uk/ukpga/2004/36/contents

Australia has the Australian Inter-Service Incident Management System, the UK has the Gold-Silver-Bronze Command Structure, and The Netherlands has the Coordinated Regional Incident-Management Procedure (GRIP), to name a few examples.

Although ICS look nice on paper, their fault lies in the extent to which they can be tested and evaluated in practice. Despite sophisticated ICS and joint protocols, many recommendations and findings from major incident reports repeatedly note the lack of coordination among services (see http://www.jesip.org.uk/why-do-we-need-jesip/). Effective ICS therefore need mechanisms which foster shared organizational learning. Examples of these mechanisms include, but are not limited to, joint training and education and co-location and co-response.

**Joint-training and Education**

To foster better coordination and shared organizational learning among the emergency services, many localities and regions develop joint training programs and simulation exercises. There are different types of training methods of varying complexity, cost, purpose and effectiveness. These range from seminars, workshops and table tops, to drills, functional exercises and full-scale exercises (Callahan et al. 2008, p.52). Today, the value of conducting exercises and simulations is highlighted in most textbooks on disaster and crisis management (e.g. Rosenthal et al., 2001; Lagadec, 1997) and mandated by legislation and executive rules in connection with a variety of natural and technological threats in most industrialized nations (Selvarajah 1993 in Perry 2004, 64).

In some countries there are examples of more integrated education initiatives among emergency service organizations. Rather than the sporadic joint-simulations, first responders receive joint training at purpose-built facilities or colleges alongside one another. A prime example of this is Singapore’s Home Team Academy (HTA). Established in 2006, The HTA is a branch of the Ministry of Home Affairs and has a number of core functions including corporate services and joint training across the emergency service agencies and other relevant safety and security organizations (Parry et al. 2015, 8). The UK’s Joint Emergency Services Interoperability Principles (JESIP) is another noteworthy joint training initiative, which has implemented a nationwide joint training strategy for all level of command11.

**Co-location and Co-response**

Co-location has become a common way in which emergency services organizations are working more closely together, although it is certainly not a novel arrangement. Co-location entails the

---

11 See http://www.jesip.org.uk/what-will-jesip-do/what-will-jesip-do
sharing of buildings and physical sites by two or more of the emergency services. There are various ways that the emergency services have chosen to co-locate. Common examples of co-location are joint emergency control rooms or centers, which house all emergency call dispatchers under one roof. More ambitious examples of co-location include the development of emergency service ‘hubs’. Poynton Emergency Services Hub, which opened in January 2014, offers police a modern facility and central location alongside the Cheshire Fire and Rescue Service and the North West Ambulance Service (Emergency Services Collaboration Working Group 2014: 4).

In addition to co-location, some departments are teaming up to respond to emergencies together. Co-response typically refers to schemes where firefighters respond to emergency medical calls on behalf of ambulance services when needed. There are other, more novel, examples of co-response schemes in the UK including London’s Joint Response Unit (JRU), and Greater Manchester’s Community Intervention Teams (CRIT).

**Shared back-office/business functions**
The main functions of emergency service organizations are supported by extensive back-office functions, or “support services” including Information and Communication Technology (ICT) development and maintenance, human resource management, equipment and vehicle procurement, estates and facilities management and vehicle maintenance, to name a few. The Emergency Services Collaboration Working Group (2014) has highlighted a number of regions in England and Wales in which the emergency services are merging back-office functions. These efforts are often alongside co-location arrangements. Surrey, for example, is piloting the Multiagency Information Transfer (MAIT) program, aimed at reducing the call transfer time between emergency services (Emergency Services Collaboration Working Group 2014: 4). On 1st February 2014, the ‘H3’ legal partnership in Hampshire was established to share corporate resources between the police, fire and county council. New developments include an integrated business center (IBC), which will provide transactional services, procurement, occupational health, property services and facilities management (Emergency Services Collaboration Working Group 2014: 24).

**Organizational integration and consolidation**
Examples of collaboration such as co-location, joint protocols and joint-training still imply an organizational distinction between the different emergency services. There are some examples of departments moving to fully consolidate their emergency services into one, multi-functional department. Stelter (2013), informed by Heinonen and Wilson (2013), outlines four forms of public safety consolidation: (i) nominal, (ii) functional, (iii) partial, and (iv) full (see figure 2). With
nominal consolidation (i), the least integrated of the forms, services are not integrated and there are no cross-trained public safety officers (Stelter 2013). Nevertheless, separate services may share facilities or training and dispatch resources and a public safety director may oversee separate services (Stelter 2013). With functional consolidation (ii), departments remain separate, and consolidation only occurs at the middle or upper management level. Partial consolidation (iii) implies the development of cross-trained public safety officers working alongside traditionally separated personnel, with consolidation limited only to select positions within the organization’s hierarchy. Finally, with full consolidation (iv), services are integrated with public safety officers fully cross-trained in both police and fire services under a consolidated management and command (Stelter 2013).

Conclusion

The emergency service sector is a complex organizational system that has evolved drastically over the past two centuries. Most pre-industrial societies relied on informal, unreliable and disjointed arrangements for maintaining public order, fighting fires and providing rapid medical aid. The great cities of the industrial revolution spurred the more systematic and formal provision of emergency services. With rampant crime, widespread disease and large and frequent fires, urban communities established professional organizations tasked with providing more effective services. The origins of these respective services have largely influenced their evolution, and the way that they are organized to this day both in the UK and around the world.

Contemporary organizational structures of emergency services are highly contextual, reflecting the historical, legal and political evolution of the societies in which they are embedded. Some countries maintain multiple municipal police, fire and ambulance services, with slightly different arrangements for less urbanized areas. Other countries have regional departments, with a different police, fire and ambulance service for every region, state or territory (e.g. Australia, Germany). As many police, fire and ambulance services developed locally, for the purposes of serving particular cities and towns, it is still common for countries to have many separate departments for each respective locality at either the regional or municipal level. As cities have grown and merged, a trend has been to consolidate various local departments into a single, national organization. Moreover, while most localities in the UK and abroad have emergency services that are publically provided, they exist among complex assemblages of public-private partnerships. There are other notable differences between the structure of each respective emergency service organization across countries, which often influence the ways that they work together at the national, regional and local levels. Overall, three basic organizational models of
municipal emergency service provision can be distinguished: the tri-service model, bi-service model and the consolidated model.

In the face of budget cuts and overall calls for a more efficient and effective public service, many governments are looking at streamlining emergency service provision through various initiatives. Common examples include shared incident command structures and protocols, co-location, joint-training, joint-procurement, shared back-office functions, co-response and complete organizational consolidation. As we move further into the 21st century, the emergency services must evolve to meet the unique demands of the age. Some of these include drastic austerity measures and public sector reform, mass urbanization and urban agglomeration, an increasingly interconnected risk landscape, environmental degradation, rapidly developing ICT, and rising public expectations, among others.

Many of these challenges will require more than just closer cooperation between the services; they will require drastic organizational change. This, in turn, will require a deep understanding of the entire system and how and why it has evolved over time. Understanding the past will help explain current organizational cultures, norms and values and structures, as perceived both by the organizations themselves, and also by the general public. Understanding other municipal, regional and national arrangements will allow for a more open dialogue in the sector, and facilitate the sharing of notable practices and technologies. In order for this to happen however, researchers should begin to analyze the organizations as a collective system or sector, rather than disparate organizations. Organizational design, public administration and technology and innovation management are among the numerous disciplines that should devote future resources to working with first responders and emergency service managers to collectively navigate the future of this vital sector.
References


Introduction

The expanding set of systems and applications became inevitable with the growth of the Internet. Physical activities have their equivalents in the digital world and the digital world enhances goods and services. Identity management is one pivotal element in the relation between physical and digital world, in the relation between physical and virtual entities. The issue of managing several identities has attracted much attention. There is an increased complexity in the use of personal information (Halperin & Backhouse 2008). Several attempts have been made recently to characterize the requirements of an identity management system, addressing the needs of both the users and organizations and governments that manage users’ and citizens identity.

There are notable challenges and complexity in managing digital identities of the online community. It is natural to expect crimes and security threats on individual and organization level in the digital world as well. A body of literature exists on IT security research and advanced technologies are established in the field. One core part of IT security is digital identity management; identifying and verifying who accesses digital resources and accordingly granting or denying access to the resource in request. The rapid evolution of wide area and networked systems created new landscape for security concerns (Flechais et al. 2004). Incidents such as system penetrations, viruses, insider abuse and other unauthorized access to resources grew in sophistication and impact. These incidents may target individuals, organizations or at a much higher level, states. Within the modern business environment, organizations commonly suffer from threats to corporate data, information technology infrastructure, and personal computing (Johnston & Warkentin 2010). On users (personal) level, there are ongoing incidents of identity thefts, frauds and potential threats and risks instigated on privacy and security of users data. In recent years the need for robust and reliable identity management systems has been widely recognized and one direction of IdM studies is towards leveraging interoperability, security and usability features of identity management (Leskinen 2012)(Glässer & Vajihollahi 2008).
The article at hand is part of an ongoing research on digital identity management and cyber security. It contains a literature review and a case study report. The literature review addresses the basics of identity management concepts and technologies. It further discusses and identifies security attacks that target digital identities. Cyber crisis in its loose sense is discussed as a consequence to security attacks. On the article’s second part, a case study conducted on adopting an identity management system to an e-Government service is presented.

The subsequent sections discuss different models, architectures, standards and technologies of identity management. Starting from the existing literature, we explore the basic definitions, common terminologies as well as some related works on technical issues, such as identity resolution, providing a review of existing work on security and identity related issues and also extending the review to a specific domain of application, E-government.

**Definitions and Basics**

For a complex notion such as digital identity (Bertino 2012) and for a young and much less defined field as Identity management (Pfitzmann & Hansen 2008), agreed upon definitions and terminologies are rare to find. The term “Identity” has varied and disperse set of definitions from different perspective and disciplines (Cofta 2008). Our discussions of identity is embedded in information system domain and thus we define and discuss about the digital identities used for identification purposes in the digital world.

Digital identity represents physical identity of an entity in the cyber world (Chehab & Abdallah 2009). These identities are used to access online services and resources from different domains such as e-commerce, finance, e-health or e-government. The notion of identification and identity management has developed through the years. The scope advanced from managing identities in a single organization with limited services and set of users to cross domain access, multiple identities and services (Alpár et al. 2011). The topic of identity management is being widely researched from various directions. The vital role of identity management is undeniable in different application domains such as criminal investigation context & counter terrorism, e-Government, e-Commerce and many more (Glässer & Vajihollahi 2008).

Table 1 presents a collection of identity management definitions that are pragmatic (or technical) and that link identity with the process of identification (cf Table 1). Several of these definitions refer to the terms Entity and Attribute. Entity and attribute are defined as follows.

- **Entity**: “An entity can refer to a person, such as a customer; a resource, such as a web server; or access, such as a proxy” (Chehab & Abdallah 2009).
• **Attribute**: A set of data that describes the characteristics of a subject. The data includes the fundamental information for identifying a subject (e.g., full name, residence and date of birth), preferences, and the information generated as a result of his/her activities. Some examples are given/family names, residences, ages, genders, roles, titles, affiliations, activity records, and reputations (Bertino & Takahashi 2010).

Table 1 below lists definitions of the terms identity and digital identity taken from the literature.

<table>
<thead>
<tr>
<th>(Pfitzmann &amp; Hansen 2008)</th>
<th>An identity is any subset of attributes of an individual person, which sufficiently distinguishes this individual person from all other persons within any set of persons.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Jøsang et al. 2007)</td>
<td>An identity is a representation of an entity in a specific domain. An identity is normally only associated with a single entity. Shared identities may exist in some sense, for example a family identity that corresponds to several people in a family unit.</td>
</tr>
<tr>
<td>(Jøsang et al. 2007)</td>
<td>A digital identity can be defined as the identity resulting from the digital codification of characteristics and attributes in a way that is suitable for processing by computer systems.</td>
</tr>
<tr>
<td>(ITU 2010)</td>
<td>A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.</td>
</tr>
<tr>
<td>(Osmanoglu 2013)</td>
<td>A unique identifier and descriptive attributes of a person, group, device, or service.</td>
</tr>
</tbody>
</table>

An identity consists of a set of characteristics, which are called identifiers when used for identification purposes (Jøsang & Pope 2005). The identifiers also known as attributes could range from name, date of birth, residential address, nationality (or country of origin) to biometrics information such as finger print, iris scan or face recognition (Phiri & Agbinya n.d.) (Bertino 2012). The attributes could also be static or changing (e.g. residential address). Examples of digital identity mentioned by Osmanoglu (2013) include user or computer account, e-mail accounts, user entries in a database table, and logon credentials for applications. An identity may depend and vary on the context the entity is in, thus, resulting in different sets of attributes representing a given individual. For instance, identity used to authenticate to online banking might be different from that of the identity used to authenticate to a social networking service (see, e.g., (Chehab & Abdallah 2009)). For this the concept of Partial identity comes into picture. (Pfitzmann & Hansen 2008) define partial identity as “a subset of attributes of a complete identity, where a complete identity is the union of all attributes of all identities of this person.”
Identity Management

Now that we have an idea about what digital identity is, let us see what identity management refers to. Identity management, IdM in short, is being defined and explained in different ways by various authors in the field. Khan and Hayat (Khan & Hayat 2009) describe IdM as a complex system that integrates different technologies, not limited to handling technical aspects but rather sociological and legal aspects as well. Wood (Wood 2005) classifies the process of identity management as two concepts; Management of identities and Management by Identities. According to Wood (2005), Management of Identities is the process of issuing and using digital identities and credentials (such as usernames and passwords). Whilst Management by Identities combines the proven identity of the user with the authorization process in order to grant access to resources. In practice, Management by Identities covers the process of establishing the identity of a remote user (or system), managing access to services by that user, and maintaining identity profiles concerning that user (Alpár et al. 2011).

Below Table 2 lists different definitions of identity management taken from the literature.

<table>
<thead>
<tr>
<th>Table 2 Definitions of IdM</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(The Burton Group, 2003)</td>
<td>“The set of business processes, and a supporting infrastructure for the creation, maintenance, and use of digital identities”</td>
</tr>
<tr>
<td>(Cao &amp; Yang 2010)</td>
<td>“IdM is the policies, rules, methods and systems that implement identity authentication, authorization management, access control, and operation audit based on digital identity.”</td>
</tr>
<tr>
<td>(ITU 2010)</td>
<td>“A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting business and security applications.”</td>
</tr>
<tr>
<td>(Jøsang et al. 2005)</td>
<td>“A process of representing and recognizing entities as digital identities in computer networks”</td>
</tr>
<tr>
<td>(Arabo et al., 2011)</td>
<td>“Identity management (IdM) deals with how users are identified and authorized across networks.”</td>
</tr>
</tbody>
</table>

Identity life cycle

A digital identity has a lifecycle; from being assigned to an entity until its disposal. In between it is used to authenticate and authorize the entity it represents and it can be maintained or revoked. IdM handles life cycle of identities in all aspects such as credential acquisition for authentication.
purpose, identity storage, verification and maintenance and terminating with identity disposal (Chehab & Abdallah 2009).

Windley (2005) states that digital identity lifecycle comprises of provisioning, propagating, using, maintenance and de-provisioning as depicted in Fig. 1. A brief description of the processes is as follows. According to Windley (2005):

a. Provisioning is the creation of the identity record and its population with the correct attributes.
b. Propagating the identity record to other systems that will use it.
c. Using once the identity has been provisioned and propagated the identity is used by various systems ranging from authentication and authorization to more complex tasks as billing and payroll.
d. Maintaining is to have some change when necessary such as attribute addition, password and re-propagate the identity.
e. De-provisioning is removing identities from the system once they are at the end of their lifecycle

We find various systems and tools; commonly known as identity management systems, that support the effective use and protection of digital identities. These systems are implemented in different models and architectures. The following sections discuss more about identity management systems.
Identity and Access Management Systems

Pfitzmann and Hansen (2008) denote identity management systems as “a technology-based administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re) used in a specific context or role.” Fig. 2 captures identity management functions as described by Osmanoglu (2013).

Components of Identity Management Systems

The purpose of identity management systems include secure and easy management of identities and corresponding attributes, handling of identification and authentication of users (Slamanig & Stranacher 2014). The following three processes capture activities and tasks involved in IdM systems. They are:

1) Identity Provisioning: refers to the process of provisioning and de-provisioning of several types of user accounts (e.g. end user, the application administrator, IT administrator, supervisor, developer, etc.) (Leandro et al. 2012).
2) Access Management: As defined by Osmanoglu (2013), Access Management refers to the processes and technology used to control the access to specific assets provided to a specific identity.

a) Authentication: To get access to any service or system one should be authenticated first. Authentication is the process of verifying the identity or other entity verifying the user, process, or device. This is done using credentials the user provides. Credentials are a subset of identity attributes that are used in verifying the entity’s identity (Chehab & Abdallah 2009). Credentials generally take the form of one or more of the following factors:

- Something the user knows, such as passwords and PINs;
- Something the user have, such as smart cards, encrypted token or a PKI certificate; or
- Something the user is which is captured by biometric characteristics such as fingerprint and iris scan.

Scholars have divided authentication approaches into two, namely, single-factor and multi-factor authentication approaches.

- Single-factor authentication is the most basic authentication approach that relies on passwords (something the user knows) in combination with a user-ID.
- Multi-factor authentication also known as strong authentication is when a combination of factors is used to authenticate users. This scheme is implemented by many high-risk systems and is generally believed to be more secure.

Biometric authentication is when users are identified using biometric data such as fingerprints, hand geometry, retina scans, iris scans, face recognition and voice analysis.

b) Authorization: Authorization is the process of verifying whether the user has the right to access the service or the requested resource. The right to access resources varies depending on the access right granted for each user of a given system. In the literature we find three common access control models.

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role Based Access Control (RBAC)

3) Directory Service: A directory service provides the infrastructure for secure identity data storage and organization. Depending on the type of data stored the three types of data repositories are:

a. Identity repository
b. Entitlement
c. Roles and rules repository

Architectural models

Over time, different identity models have emerged, having differences in terms of user control or identity data storage (Slamanig & Stranacher 2014). There are three main models being discussed in literature:

- Isolated model
- Centralized model
- Federated model

These three models are being described more in detail in this section.

**Isolated Model**

Cao and Yang (2010) describe an isolated model as a model where SP plays the role of service provider and identity provider. A single server performs storage and all identity and user operations. Its advantage, according to Ahn and Ko (2007), is that this model is simple to implement. The disadvantage is that loss or forgetting credential cost the SP if secure implementation is needed, that Centralized storage might lead to problems such as single point of failure, identity theft and privacy protection issues. Fig 3. depicts an isolated model where SP acts as both SP and IdP.

![Isolated-IdM model (Cao & Yang 2010)](image)
**Centralized model**

This model is implemented in a client-server mode where user identity storage and user authentication are both implemented on the same server called Identity Provider (IdP). Different from isolated model, the centralized model separates the tasks of IdP and SP.

![Centralized -IdM model (Cao & Yang 2010)](image)

As described by Cao and Yang (2010), it is suitable for the requirements of managing a lot of users. But, unlike federated models, the centralized model requires all users to be in the same domain. Cao and Yang (2010) further mention that the model’s feature of storing all identities in only one IdP and not supporting cross-domain access is a disadvantage of using this model.

**Federated model**

As defined by Maler and Reed (2008) federated identity management is “a set of technologies and processes that let computer systems dynamically distribute identity information and delegate identity tasks across security domains.” Similarly (Jøsang et al. (2007) describe federated model as a set of agreements, standards and technologies that enable SPs to recognize user identities and entitlements from other SPs. Federated identity is the means by which web applications can offer users cross-domain single sign-on (SSO) feature. This technology allows users to authenticate once and thereafter gain access to several services. The principle behind the federated model is supporting cross-domain access and entertaining multiple domains.
Federated systems are widely employed in corporate and academic environments. This model increases the value of user credentials (as it provides access to more resources) (Dhamija & Dusseault 2008).

In federated models the coordination between SPs and IdPs is on the basis of trust. As illustrated in Fig. 5 SPs trust different IdPs in verifying user identities.

Several authors and domain experts agree on the advantages of using federated systems. It allows interoperability across organizational boundaries and connects processes utilizing different technologies, identity storage, security approaches and programming models. Within a federated system, identities and their associated credentials are stored, owned and managed separately. Each individual member of the federation continues to manage its own identities, but is capable of securely sharing and accepting identities and credentials from other members' sources. In this model the SP and IdP are separate organizations and their cooperation is based on trust (Chehab & Abdallah 2009).
A comparison of the three models

The following table is from Cao and Yang (2010). It compares the three models discussed above. As can be seen from Table 3, isolated model supports integrated single SP, which is the IdP as well. Unlike the isolated model federated and centralized models support multiple SPs but in the case of centralized Single IdP is supported with little support to multi services from multi domain access.

<table>
<thead>
<tr>
<th>Model</th>
<th>SP Type</th>
<th>IdP Type</th>
<th>Service Composition</th>
<th>Cross Domain Access</th>
<th>Identity Storage</th>
<th>User Control over Identity</th>
<th>Privacy protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolated</td>
<td>Single SP and IdP, SP is IdP</td>
<td>Single IdP and SP, IdP is SP</td>
<td>Sole service</td>
<td>No support</td>
<td>On SP</td>
<td>No control</td>
<td>Few and very weak protection</td>
</tr>
<tr>
<td>Centralized</td>
<td>Multi SPs</td>
<td>Single IdP</td>
<td>Multi services but in the same domain</td>
<td>Limited support</td>
<td>On IdP</td>
<td>Few control</td>
<td>Much but weak protection</td>
</tr>
<tr>
<td>Federated</td>
<td>Multi SPs</td>
<td>Multi IdPs</td>
<td>Multi services from multi domain</td>
<td>Nearly full support</td>
<td>On both SPs and IdPs</td>
<td>Much control</td>
<td>Much and strong protection</td>
</tr>
</tbody>
</table>

Currently the widely adopted and implemented model is the federated identity model. It supports multi SPs, multi IdPs and cross-domain access (see Table 3). Although this model is widely implemented and used there are some shortcomings of the model as pointed out by many authors in the field. An example is the single layer of authentication decreasing system security (Alpár et al. 2011). Current federated approaches to digital identity management do not adequately protect individuals from identity theft, as stated by Bertino et al. (2010), where fraudulent individuals can register stolen identifiers or impersonate other individuals.
Paradigms of IdM systems

Based on the development stage of IdM and transfer of IdM core subject Cao and Yang (2010) present three paradigms of IdM, namely, Network centric, Service centric and User centric paradigm.

In network centric paradigm identity creation, management and deletion have nothing to do with the access or entitlements as described by Cao and Yang (2010), rather the IdM system is established and operated by a single entity for a fixed user and resource community. It’s not service-related or user-related. Service centric paradigm IdM is composed of services from different providers across multiple domains; these services are not necessarily under control of their providers. In service centric paradigm IdM, organizations will evolve their systems to provide more and more services, so IdM can offer a broader range of applications (Cao & Yang 2010). User centric IdM paradigm, on the other hand, shifts the control of digital identities from SPs to the users by putting the users into the middle of transactions between identity providers and relying parties.

<table>
<thead>
<tr>
<th>Paradigm</th>
<th>Centralized Trust Domain</th>
<th>Identity Handling</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Authentication</td>
<td>Identity Number Scale</td>
<td>Identity Uniqueness</td>
<td>Credential Transmission</td>
</tr>
<tr>
<td>Network Centric</td>
<td>Centralized</td>
<td>Sole</td>
<td>Single Method</td>
<td>Small scale</td>
<td>Unique; a single identity</td>
</tr>
<tr>
<td>Service Centric</td>
<td>Centralized combined with partly distributed</td>
<td>Multiple</td>
<td>Support of many centralized and few distributed methods</td>
<td>Large scale</td>
<td>Unique; Main identity and some affiliated identities</td>
</tr>
<tr>
<td>User Centric</td>
<td>Centralized combined with distributed</td>
<td>Multiple</td>
<td>Support of centralized and distributed methods</td>
<td>Large scale</td>
<td>Unique; Main identity and some affiliated identities</td>
</tr>
</tbody>
</table>
**Popular IdM Initiatives**

Table 5 summarizes some examples of projects and initiatives in identity management.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIDIS <a href="http://www.fidis.net">http://www.fidis.net</a></td>
<td>A global consortium of more than 150 companies to develop an open standard for federated identity based web service.</td>
</tr>
<tr>
<td>Liberty Alliance <a href="http://www.projectliberty.org">http://www.projectliberty.org</a></td>
<td>The Liberty Alliance is a consortium founded to develop an open standard for Federated identity model.</td>
</tr>
<tr>
<td>PRIME <a href="https://www.prime-project.eu">https://www.prime-project.eu</a></td>
<td>A European initiative for management of the multiple identities a consumer may have obtained through his online interactions.</td>
</tr>
<tr>
<td>OpenID <a href="http://openid.net">http://openid.net</a></td>
<td>A framework handling many identities of same user across different websites.</td>
</tr>
<tr>
<td>Shibboleth <a href="https://shibboleth.net">https://shibboleth.net</a></td>
<td>An open-source project that provides Single Sign-On capabilities and allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner.</td>
</tr>
<tr>
<td>Higgins <a href="http://www.eclipse.org/Higgins">http://www.eclipse.org/Higgins</a></td>
<td>An open source Internet identity framework designed to integrate identity, profile, and social relationship information across multiple sites, applications, and devices.</td>
</tr>
<tr>
<td>Forgerock products <a href="https://www.forgerock.com">https://www.forgerock.com</a></td>
<td>An open source Identity Relationship Management solutions and platforms that extends across cloud, social, mobile, and enterprise environments.</td>
</tr>
</tbody>
</table>

**Crisis situations and challenges in IdM**

This section provides an overview of cyber crisis situations and challenges in Identity management.

**Privacy**

Privacy is among the debatable issues in identity management that has gained a lot of attention recently. Various authors wrote on privacy, how to preserve it, technologies to help preserve privacy and related topics to enhance privacy in the digital world. Many researchers and practitioners are working towards bringing privacy preserving technologies and solutions. Jendricke and Gerd (2000) state that the most challenging issue in Identity management is privacy and requirements related to privacy impose fundamental restrictions on the design and effectiveness of the systems.

Alpár et al. (2011) study shortcomings in existing identity management. They list trust, privacy and security issues as shortcomings and further argue that the current design of IdM systems
need to address these limitations before considering the systems as fully secure, privacy friendly and usable.

Various initiatives and projects on identity also focus on enhancing privacy. PRIME (https://www.prime-project.eu) and PrimeLife (http://primelife.ercim.eu) are examples of European research and development projects that aim to contribute to online privacy.

**Security requirements and architectures**
The guiding principle behind any security architecture of a system is ensuring confidentiality and integrity of data and availability of the system at all times (Malone & Siraj 2008). Data should be protected, as it is a valuable resource for users as well as organizations. Systems must be protected as well to ensure their degree of intended availability but not overly constrained by security measures that might obstruct normal operations. When systems are designed, security requirements are also considered that are expected to be implemented with the system. This also holds while designing and implementing Identity Management systems.

Definitions of some notions used quite often: Fabian et al. (2010) define security goals as very general statements about the security of an asset. Security requirements capture security goals in more detail. A security requirement refines one or more security goals (also indicates the counter stakeholder against whom the requirement is directed.).

There are a number of generic and mature architectural evaluation methods for software architecture design decisions. For IdM Staite and Bahsoon (2012) proposed a method to guide and assist in selecting a secure identity architectures. In their work they used qualitative and quantitative metrics for evaluating identity architecture. Glässer & Vajihollahi (2008) proposed a semantic model called *Identity Management Architecture*, for analyzing and reasoning about identity management concepts and requirements. Satchell et al. (2006) argue that solution providers should look more and beyond security when providing federated IdM systems. They further argue that user control and personalization should be incorporated in the design of the systems. Damiani et al. (2003) underline that digital identity solutions should support at least three requirements i.e. Reliability and dependability, Controlled information disclosure and Mobility support.

**Cyber Security and Cyber Attacks**
Being able to verify the identity of individuals, organizations or devices is a primary requirement in cyber security as access to any resource starts from verification of the requesting body. Cyber security in general deals with the protection and security of assets and resources in the cyber
realm. Following, cyber security attacks that mainly target digital identities and their effect on individuals and organizations are discussed.

- A (cyber) incident is a disruption of IT services where the expected availability of the service disappears completely or in part. It can also be the unlawful publication, obtaining and/or modification of information stored on IT services (ENISA 2014).
- A serious threat to the basic structures or the fundamental values and norms of a system (in cyberspace), which, under time pressure and highly uncertain circumstances, necessitates making vital decisions (ENISA 2014).

Cyber-attacks as a threat to business and national security have become one of the pressing concerns to organizations and governments. These attacks are increasing both in number and capacity to cause serious operational and financial damage. Threat is defined as a potential violation of the system security (Newman 2006). Among the demands of building a secure system is having an up-to-date knowledge of security threats (Flechais et al.). This is vital as the nature and complexity of threats and cyber-attacks is changing through time. Such attacks are carried out by three categories of people. Namely:
  - Hacktivists – politically motivated groups
  - Organized criminal groups
  - State sponsored groups

A stream of literature is available on information and systems security threats. In this section those security issues identified targeting digital identities is discussed. Here are some of the threats on digital identities found in the literature:

- Information disclosure is a threat that occurs whenever some confidential element that is stored on a network resource or in transit between a network resource is compromised to someone not cleared to receive such information (Newman 2006).
- Identity theft and fraud to impersonate a legitimate user: Glässer & Vajihollahi (2008) state identity theft as the misuse of another person’s identity information. It generally refers to malicious parties stealing individuals’ passwords or credentials for financial gain or other purposes (Bertino 2012).
- Phishing: this is an attack aimed at stealing sensitive personal data that can lead to committing online economic frauds. The information could be username and password, credit card details, and the like by masquerading trustworthy entity in an electronic communication.
- Large scale spoofing: this attack is aimed at identity theft. It describes a situation where one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
• Misplaced trust: is a treat that describes a situation when a trusted entity abuses the trust for malicious purpose (Chehab & Abdallah 2009).
• Social engineering: is the art of manipulating people into performing disclosure actions or divulging confidential information.
• Malicious use of privileged access (accounts).
• Brute force attacks.
• Password compromises of SSO systems.

According to PWC (2011) attackers are motivated by one or more of the following goals:
• Leaking sensitive customer information to the public for financial gain or to harm the organization.
• Significant disruption of business operations.
• Leaking sensitive corporate information to the public to damage a company’s reputation.
• Stealing sensitive corporate information for profit.
• Obtaining and maintaining control of critical infrastructures.
• Maintaining remote access to systems for a long time to re-compromise networks.
• Stealing personal customer data, including card data and identity information, to resell in the criminal underground for financial gain.

The consequence of the attacks could be various. For instance, it could result in unauthorized access, misuse of data, disruption of services, or any combination of these situations or damages.
• Financial Loss: Security breaches on identity and access management cause up to billions of dollars of financial loss each year, both reported and unreported (Dhamija & Tygar 2005). In 2005 for instance an identity theft of 8.3 million people happened as reported by (Anderson, Durbin, & Salinger, 2008).
• Damage on reputation: Reputation is a valuable asset to an organization. As a good reputation is vital for a business a damaged reputation can cause loss of customers and investors or partners. A survey made by PwC indicates that reputational damage is the biggest fear of 40% of respondents while experiencing cyber security incidents (Pwc 2011).
• Damage on Business.
• Legal consequence.

Crisis
According to Larkin (2011) crisis is “an inherently abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation or existence of an organization.” Global standards body, BSI Group, defines a crisis as an abnormal and unstable situation that threatens an organization’s strategic objectives, reputation or viability. In its loose sense, herewith cyber
A crisis is referred to mean undesired and unstable situations that are caused by cyber-attacks. Kulikova et al. (2012) state that cyber crisis has unique features that are different from a physical crisis. In some cases, the severity of cyber crisis is high but confined to individuals or few organizations in a limited area. In other cases the severity may be low but widely spread to a larger area. The following diagram depicts a cyber crisis management model.

**Case study: Forgerock as Identity Management System for eGovernment Service - Bürgerservice-Portal**

Proper and secure management of users’ identity is crucial for any type and size of organization. This case study describes an implementation and adoption of identity management system for an eGovernment portal called Bürgerservice-Portal based on a software package called Forgerock. The project was designed to be a feasibility study – to explore whether Forgerock products will meet the specific requirements of the Bürgerservice-Portal and improves the current functionalities of the system’s security and access control. This portal has its prior identity management functionality intact. The study was also conducted to provide information about capabilities needed for customizing and integrating Forgerock as well as the resources necessary for the full integration. The study also extends to see the possible advantages of Forgerock over the existing individual identity management solution used in the eGovernment system.
Method
A case study, as defined by Eisenhardt (1989), is a research strategy that focuses on understanding the dynamics present within single settings. The case study follows guidelines of P. Schubert et al. (Schubert & Wölfle 2007) and eXperience online (www.experience-online.ch).

The Context: e-Government and eID in Germany
This section provides some information about the context of the case study, e-Government and its special requirements.

e-Government

e-Government is defined as “the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government” (Information for Development Program 2009). E-government services are distinct from private sector services. The difference is mainly due to the fact that public institutions must look into much broader issues such as interoperability, inclusion and consistency as it serves the entire population (Baldoni & Antonio 2009).

Secure management of the citizens’ identity is vital for e-Government, which has elevated security requirements, as the data stored on governmental level is sensitive information. In the past few years, different governments of various nations have introduced electronic card-based citizens’ identification systems to physically & digitally identify citizens and to improve secure authentication. To name some, Italy, Germany, Denmark, Belgium, Austria, UK are examples from EU member nations that implemented the electronic identification card (eID) system. The implementation of the system could differ depending on the governmental structure, legal issues, political and economic status, and socio-cultural values of the country. E.g., in Germany, the current legal context requires all institutions to have their own certificate and identification infrastructure in place. Different governments have their version of e-Government processes and infrastructure. For instance, according to Germany’s governmental structure, the local municipalities have almost full autonomy in regard to providing public services (Noack & Kubicek 2010) which may not be the case in other countries.

Electronic identification card system
The Electronic identification card (eID) is a portable cryptographic card, nearly the size of a credit card, with a built in chip widely used for digital security purposes. Being among strong authentication mechanisms (strategies), these cards are used to perform secure payments and
provide secure documents such as passports and identity cards. This technology has been used for many purposes. In addition, several governments have utilized this technology for identification purpose (both physically and digitally) of citizens and other residents. Smart cards allow for a trustworthy execution of authentication functions and other cryptographic operations. Klenk et al. (2009) argue that with the current government efforts towards electronic identity cards (eID) a new generation of trustworthy smart cards emerges that will have a very broad deployment and can be used for a verified authentication of users towards services or an Identity Provider.

Al-Khouri describes that governments in the last decade have spent great efforts and substantial financial expenditure in modernizing their identity management systems with the aim to develop compelling Identity Profiles to strengthen secure systems and protocols used across government agencies (Al-Khouri 2012).

**e-Government and eID in German context**

As Noack and Kubicek (2010) describe, in the late 1990s public services in Germany began to be offered via Internet. But for legally binding transactions such as in tax payment process the person has to physically be present at the offices for the signatures. In 1997, Germany passed a new law about a framework for electronic signatures where after two years the federal government granted a fund for the local municipalities to develop legally binding online public services with e-signatures. After the implementation there was an issue regarding the attributes used to sign electronically. The attributes were only last name and first name which one can find redundancy in. Thus they were not sufficient to uniquely identify a person since there could be more than one citizen with the same first and last name. After the September 2001 attacks, amendments were made to the law to include biometric information of citizens on the personal ID (Noack & Kubicek 2010).

Enhancing the e-Government sector in Germany has continued. Although digital identification of citizens was introduced, until 2006 the issue of online authentication was not very well addressed. In November 2010, Germany has introduced online authentication as one feature of the new electronic Identification card (eID). Smart cards allow for a trustworthy execution of authentication functions.

Germany has a federated governmental structure. There are 16 federated states and more than 5000 local municipalities. Noack and Kubicek (2010) state that according to the law of the land, the local municipalities are almost autonomous and they are in charge of registration and administration of their respective residents at the local registration offices. But the local registered data is sent to an integrated state level database for 24h availability for police access.
(Noack & Kubicek 2010). According to the German data protection law it is prohibited to use or process more information about a person than needed for a particular purpose. So access to identity data is restricted. Government agencies can get access to the data either from the machine-readable part of the card or from a certified card reader by the consent of the cardholder. The consent is given by entering the PIN code on the card reader. Exception to this rule is to sovereign authorities with certified reader. This body can access identity data including biometric information without the PIN of the card holder (Noack & Kubicek 2010).

**The Motive for the Case Study**

The design study was motivated by a business need and forecasted benefit in having independent identity and access management system. Identity management system handles user provisioning, access management and related processes regarding overall management of users’ digital identities. For this the Forgerock software package was chosen and tested to see whether it fits the requirements of the current Bürgerservice-Portal- an eGovernment portal.

H&D plans to expand its eGovernment business and considers cost efficiency and sustainability key selling propositions of eGovernment solutions in its consulting and system business. H&D considers the use of a standard software of identity management to be one step towards more cost efficient and sustainable solutions and also towards a system architecture with which eGovernment systems would be able to react in an agile way to cyber threats, new legal requirements, novel technology trends or user requirements. With the move to Forgerock as an implementation platform for identity management, H&D has various objectives.

First H&D is considering becoming Forgerock’s partner in Germany and sees this as a strategic move in the German eGovernment application market. The internal project has the aim to validate the maturity and functionality of Forgerock for the applications that H&D created.

Forgerock is a relatively young company founded in 2010 with products available since then. It develops open source identity and relationship management solutions that extend to cloud, social, mobile, and enterprise environments. Customer case studies at the platform report successful adoption of Forgerock to e-Government. Examples on this are the government of Norway and Canada. Government of Norway testimonial says by using Forgerock product, the Government of Norway is able to save millions and improve quality of government services with secure single sign-point access to more than 300 government services.

“*By providing simple, secure access to government services, the OpenAM solution has played a large part in the success of the eGovernment initiative.*”

---

75
By centralizing the authentication process on OpenAM’s flexible and open architecture, the Norwegian government is able to make the most of its resources.” (Tor Alvik, Norway’s Agency for Public Management and eGovernment  https://www.forgerock.com/en-us/resources/)

Studying and experimenting how enterprise software package can be utilized by e-Government applications is expected to bring two major advantages. First, cost reduction in implementation, maintenance and management as it is a typical advantage of using standard software. Almost all systems have an identity management functionality implemented since it is the core part in securing any system. The cost, on the other hand, of implementing or integrating security features to such built in systems is undesirable. Using identity management system can lower the cost of integrating security features, which would rather readily come along with IdM systems. Second, H&D sees various advantages in providing standard identity management features to its e-Government service provider clients and their users. Enterprise identity management systems are available in the market and these systems are solely developed to handle digital identity management processes. The systems also incorporate state of the art standards and means when it comes to security and privacy issues. Using or adopting such systems offers the features that are desired to have in managing identities. Which in turn simplifies in-house implementations and integration efforts.

The Project Structure

Team composition and implementation methodology
A team of three graduate students and one undergraduate student was responsible for the implementation work. Two additional participants, one senior IT expert and consultant (ITE) and a senior software engineer (SE), from H&D were involved during the entire process of the project. The team followed the Scrum method of agile software development in the project where the Scrum elements task division, peer-programming, and daily standup meetings were all part of the process.

The fundamental roles of the Scrum method are Product Owner, ScrumMaster and the Team. In our study ITE played the role of product owner by leading the development process and providing support and guidance to the team. SE played the role of ScrumMaster by facilitating the development process and in helping solve difficulties and impediments whenever necessary. The daily standup meetings were part of the study as well. These meetings were held in presence of ITE, SE and all team members and are usually short. It created a favorable venue for discussing business requirements, project progress and difficulties among the team members and project participants.
Time frame and project milestone

The design study was carried out in a period of five weeks. The team used the first few days to set up the infrastructure and familiarize ourselves with the software tools to use in the study. Afterwards the implementation was done in an agile process. The tasks were divided among team members whereby each member addresses the tasks either individually or together with another member whenever necessary.

The major milestones of the project were:

- The first milestone was software installation, configuration of the tools and getting familiar with the tools to use. This included:
  - OpenAM deployed on Tomcat web container
  - GateIn portal to run on JBOSS server
  - OpenIDM configuration
  - OpenDJ configuration
- The second milestone was addressing the specified business needs in an incremental manner. The team worked in bringing the solutions for the requirements and tasks were divided among the team members whenever necessary.
- The third milestone was the implementation of the central repository. At a later stage of the study, a central repository was configured to organize and merge the individual components into one solution.

Stakeholder presentation and stakeholder analysis

Stakeholder H&D GmbH

The primary stakeholder and initiator of this study is Unternehmensberatung H&D GmbH, a business consultancy firm based in Germany for over 20 years. H&D serves the entire spectrum of organizational consulting, application-based software development, and accompanying services in information technology.

In addition to developing solution concepts, H&D extends its services to assist clients with implementation during the early stages, training users and providing the expected customer service and support as well. The focus areas include:

- Process analysis
- Organizational consulting
- System architecture and software development
- System integration and migration
H&D works closely with the German government on e-Government services. Through the years, H&D participated in various e-Government initiatives and projects. Since the last decade, the Federal Government of Germany provides full support to widespread adoption of e-government services and works towards making Germany one of the leaders of e-government in Europe. Nevertheless, studies show that there are challenges in adoption of online public services by citizens. The study further shows that among the factors affecting the adoption the highest percentage (86.6%) are factors of data protection, privacy and security followed by reliability of systems (85.7%) (Akkaya et al. 2013).

**Decision in Favor of Forgerock (www.forgerock.com)**

Selection of an identity management solution may not be easy and it requires a comparison of features and functionality that best fits the organization’s needs, preferences and budget. The selection of the software packages and tools were done and provided to the team by the stakeholder company. The criteria for choosing the Forgerock as an identity management system for this study are:

- Cost: Open source, thus free to download and customize
- User interface- simple and customizable user interface
- Customizable feature of the products to fit specific business needs
- Partnership with Forgerock for future collaboration

Forgerock offers identity and access management services through its four products. In our study, the software adoption and implementations are based on three of these products. The products of Forgerock are:

i) **OpenIDM** - this product deals with user provisioning, password management and identity life cycle. OpenIDM architecture includes:
   - User provisioning
   - User self-service enabling registration, password reset, and self-service access requests
   - Password management to control password use and enforce policies, giving added protection
   - Synchronization/reconciliation of customer identity data that ensures accurate information is available across all lines of business and systems
   - Customizable workflow engine
   - Cloud connectors that extend trusted, on-premise IAM frameworks into the cloud

ii) **OpenAM** - Access Management
   This product is a unified access management software that provides authentication, authorization, federation, security and entitlements. OpenAM architecture includes:
   - Authentication
• Entitlement management that enables users to access applications and services based on permissions and policies defined by the business
• Federation and single sign-on: with a single identity, allowing users to access services that span the cloud and mobile devices, on premises and off, eliminating the need for multiple passwords, user profiles, or the complexity that creates friction and slows adoption
• Social sign-on that supports integration with “sign up and log in with social media accounts.

iii) OpenDJ- Directory Service
This product is a directory service that is used to store identity and entitlement data.

iv) OpenIG- Identity Gateway
This product provides a standard-based approach to extend access to web applications and application programming interfaces.

Fig 7. Forgerock solutions (www.forgerock.com)

Decision in Favor of the German eID and the AusweisApp
An Electronic Identification card (eID) is a portable cryptographic card, nearly the size of a credit cards, with a built in chip widely used for digital security purposes. Being among strong authentication mechanisms (strategies), these cards are used to perform secure payments and provide secure documents such as passports and identity cards. This technology has been used for many purposes. In addition, several governments have utilized this technology for the
purpose of identification cards to uniquely (both physically and digitally) identify citizens. In November 2010 Germany has introduced the new functional electronic ID card nationwide.

The analysis and selection of the technology to use for the study was done by H&D as they decided to continue a successful implementation history with the software products from Governikus from their past experience.

![Sample German eID card](image)

The AusweisApp2 (www.ausweisapp.bund.de) and the Governikus-Authent Software Kit were used in this study for implementation purpose as well as to communicate with the eID test server. This application is certified by the German Federal Office for Information Security (BSI) and is available for free download. It supports Windows 7 and 8 and OSX operating systems. Recent versions support the mobile operating systems Android and iOS as well.

The AusweisApp2 is used to authenticate cardholders in the eID server. The communication between the eID client i.e. AusweisApp2 installed on the user’s (cardholder’s) machine is via Internet. A card reader is used for the communication between the user (cardholder) and the AusweissApp2. When a user inserts his/her eID card in a card reader, which is connected to his/her computer, the application will detect the card and the user is prompted to insert a PIN for authentication. This PIN is issued to a cardholder together with the card or on request to respective authorities.
Governikus KG is the provider of the eID client application software called AusweisApp2. According to the current infrastructure of the German eID a communication between cardholders and eID server is possible via eID client applications. Among the few accredited providers of such software is Governikus KG. Governikus is a private public partnership owned by four partners: Freie Hansestadt Bremen, Telekom Deutschland GmbH, Die Sparkasse Bremen and Brekom GmbH (EWE Gruppe) with products and services around secure communication in the eGovernment sector. Governikus is considered a trustworthy provider for sustainable e-Government solutions and leading provider for eID card technology.
The Bürgerservice-portal and its IdM System

We now describe the state of the system for which the adoption is intended to. The system is an e-Government portal that offers various online services for citizens and holders of the new identification card, the eID card. The services are offered municipality wise. Users can register on the portal of their municipality to access and make use of the available services. Services offered at the Bürgerservice-portal include: driving license registration, birth and other official certificate request.

The basic IdM process of the system includes registration and access management. Registration is the first basic step in identity management workflow of the system. The system also allows access to the system using the eID card without registration. In this case the portal reads the user data from his/her eID card and creates a temporary account, which is deleted when the session expires. Users who want to have a permanent account can register themselves on the portal and access the resources. The registration and access management processes of the system are described as follows:

a) Registration
To access the services, users register themselves on the portal. Two options are available for registration:

- Registration using username and password
  This process registers users who want to use credential to login to the system. On registration, among other information such as full name, birth date and address, users also provide user name and password.
- Registration using electronic id card (eID)
  This registration type is for those who want to use their eID card for providing the information needed for registration purpose.

b) Access management
Access management combines the process of authentication and authorization. Authentication is the process of verifying the identity or other entity verifying the user, process, or device. This is done using credentials the user provides such as password, PIN, smart cards, encrypted token, PKI certificate or any combination of these. While authorization deals with controlling which resources to allow authenticated users to access and make use of. Accordingly, registered users on the portal can login and use the services of their desire. In a similar manner to the registration process, the portal provides two options for logging in to the system.

- Login using username and password
  This option is using the most common means i.e. by providing legitimate credentials as username and password.
• Login via electronic identification card
   The second option is using an electronic id card (eID).

Note that we find strong authentication being implemented in this system since a combination of PIN and eID card is used to authenticate users. Note furthermore that single sign on (SSO) is another feature of the Bürgerservice-portal. Systems with SSO feature allow users to login once and access multiple services that are under the trust zone of the services.

**The new system – IdM by Forgerock in the Bürgerservice-portal**

Our project was based on the arrangement and integration of various components together since the objective was to use Forgerock as an independent IdM system. The adoption and implementation of the system was an incremental and agile process. The first step was to analyze and find out the existing systems functionality and understand what is expected of the new configuration.

**Business Requirements**

The new configuration is expected to support, functionality wise, existing system’s user provisioning and access management features. As indicated above, the existing system comprises of two options for user data registration and accessing the system, i.e. login process. Although that is the case, Forgerock components met only some of the functionalities needed. Except for the readily available use cases the rest were implemented and integrated to be functional with the Forgerock products. These additional requirements were divided among the team members for implementation.

Table 6 summarizes the requirements identified to be met by the new configuration of the system and which product will handle what function.
Table 6. Identified Requirements

<table>
<thead>
<tr>
<th>No.</th>
<th>Requirements</th>
<th>Description</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access Management/control</td>
<td>Authentication and authorization of users using Username and Password to access the portal</td>
<td>OpenAM</td>
</tr>
<tr>
<td>2</td>
<td>User provisioning</td>
<td>Registration of users handled by OpenIDM</td>
<td>OpenIDM</td>
</tr>
<tr>
<td>3</td>
<td>Signin via nPA/eID</td>
<td>In addition to the username and password login, to enable users to use their eID cards for login purpose.</td>
<td>Implemented Login Module on OpenAM</td>
</tr>
<tr>
<td>4</td>
<td>Email verification after registration</td>
<td>To confirm registration and activate the user account.</td>
<td>Implemented Module on OpenIDM</td>
</tr>
<tr>
<td>5</td>
<td>Registration via nPA/eID</td>
<td>To enable users to use their eID cards for first time registration.</td>
<td>Implemented Module on OpenIDM</td>
</tr>
</tbody>
</table>

Among the requirements listed in Table 6, Requirement number 1 and 2 were easily adopted from Forgerock products as they readily accommodate the requirements for the new system. However there were others that needed additional customization effort to satisfy the expected functionality. For this the open source nature of the platform was advantageous as it allows developing and integrating the plugins with the already functioning products for customized use. Thus modules were implemented as plugins that extend the open source nature of the platform.

System overview
The new implementation has two major blocks- Identity Provider (IdP) and Service Provider (SP). In identity management, the term IdP is used to refer to a component that handles processes such as identity creation, provisioning, and password management. Forgerock products play the role of Identity provider in the new architecture. The three products i.e. OpenIDM, OpenAM and OpenDJ are integrated to handle the overall identity and access management processes of the identity provider side.

OpenAM comes with embedded OpenDJ. However it also supports and can be configured to use other Lightweight Directory Access Protocol (LDAP) servers. For simplicity and convenience, we used the already available and embedded OpenDJ with configuration adjustments. It was configured to serve as a directory service that can be accessed both by OpenAM and OpenIDM for identity data storage (see Fig. 11). As depicted in Fig.11, OpenAM with the embedded OpenDJ deployed on Tomcat server together with OpenIDM play the role of IdP while GateIn portal plays the role of SP that consumes output of identity related outputs from the IdP.

Fig.11 depicts overview of the system.

84
OpenIDM manages the user provisioning aspect, which includes registration, password management, etc. To make OpenAM operational it was deployed and configured on Apache Tomcat web application container. After the deployment OpenAM is accessed via web browser using the deployment URI.

The e-Government portal plays the service provider role. It is represented by a fresh installation of GateIn portal on our development environment. For development and testing purpose, GateIn portal running on JBOSS server was used. GateIn is an Open source website framework that comes with various rich features for website design and implementation.

**Use Case 1: User Registration**

This use case handles first time self-registration of users to the system. The User provisioning is handled by one of the Forgerock products - OpenIDM. The two modes of registration that are being used by the existing system are also required to be functional in the new adoption. Registration via username and password option of the OpenIDM product is readily available and was easily adopted. OpenIDM provides customizable user registration functionality. In addition to the default information fields, it can be customized to add more fields for entering user information.
**Use Case 2: Email verification**
This use case implements email verification of self-registered users. Email verification is performed to make sure the email address provided during registration is valid and live. OpenIDM has a custom-end point feature to include email verification process. However, full implementation of the feature is not available in the OpenIDM. Thus a team member implemented and extended this use case to fully perform the verification task. The use case checks for validity of the email address provided during the registration process and sends out an email. After the user receives and confirms via the link provided in the email, the account is activated for further use.

**Use Case 3: Access Management**
This use case handles authentication and authorization of users for GateIn portal. OpenAM comes with a default feature for logging in with username and password. It is also possible to configure OpenAM for social logins such as via Google and Facebook accounts. In addition, the Single Sign On plugin enables seamless integration between GateIn Portal and the OpenAM Single Sign On Framework.

For more options, OpenAM offers different types of authentication module implementations for authentication purpose. It also allows implementing custom modules as plugins for additional requirements than the provided ones. The plugins then integrate with OpenAM. We used this feature of OpenAM to implement a module that accommodates the two login options. The implemented module is integrated with OpenAM. Its functionality is to run on top of OpenAM providing the user to choose the login mode, i.e. via username and password or via eID card. The two login options are discussed below:

- **Using username and password**: This use case is instantiated when users want to login to the portal. Upon request for login, the system redirects users to OpenAM where they provide their credentials. The system prompts the users with two options for logging in to the system; using their username and password or using their eID. After providing the credentials the users are redirected back to the portal on successful login. The two login options are discussed below:
(a) Using eID/nPA (electronic identification card)

The second option for signing in to the system is using the electronic identification card (eID). Thus far, this feature is not readily available in the OpenAM package. For this a module was implemented that aims to serve as an interface between OpenAM and the GateIn portal. An interface module was implemented that serves as a communication means between OpenAM and the eID client application, AusweisApp2 (see Fig. 3).

The GateIn portal keeps track of its users on its internal database that is different from the OpenAM data store. The module creates users to GateIn database, if the user does not exist, but has been authenticated via OpenAM. This usually happens, if a user logs in
with the eID. The user is authenticated within OpenAM, but GateIn lacks this information about the user. Thus, the plugin looks if a user with the same ID already exists and if not, it will be created. Afterwards, the user is logged into GateIn and can use all its features.

Fig. 13: Use case- Login via eID/nPA
**Experience**
IDM systems are built to leverage and simplify the burden of managing lots of digital identities in companies of all sizes. In most cases organizations have an already working automated system running in their context. But when it comes to adopting and shifting to the new system, it may not be as seamless as it sounds. In this project, we noticed that the business needs of the stakeholders were not fully entertained by the IdM product used in the project. Thus as a first phase implementation, we strived to meet the needs by using simple customization of the products, up to code level implementation using software APIs from the platforms as well as integration between the components. This was possible due to the open source nature of the platforms chosen for the study.

**Expected Benefits and Success Factors**
A well-implemented identity management system improves security. It also brings business benefits to organizations by reducing cost and improving service levels. IdM systems bring state of the art security features implemented in them which in return reduces the IT operational costs for integrating and implementing such features whenever necessary.

**Conclusion**
In this article we introduced one of the core parts of cyber security- identity management. We also introduced various technologies, models and architectures of identity management systems. Security and privacy aspects of digital identity were also discussed, as these are debatable and critical aspects regarding the digital information and experience of today. We further discussed a case study of an e-Government service and identity management system integration effort. The output of the project was tested only in a production environment and deployment of the system was not included in the study.

We plan to continue the work by focusing on security issues associated with the system by doing threat and risk analysis on the system. This will allow us to analyze the kind of threats the system might be facing in its real time deployment. The analysis will build upon the work of Paintsil (2013) who introduced an executable model based risk analysis method for identity management systems. The method is called EM-BRAM and it identifies risk factors inherent in IdM systems and uses them as inputs for privacy and security risks analysis.
References


Phiri, J. & Agbinya, J.I., Using Artificial Neural Networks to Implement Information Fusion in Digital Identity Management Systems.


Assessing Police Use of Social Media Technology – A Case Study on Online Communication by the Greater Manchester Police

Kieran Lewis

Abstract

This chapter will explore the topic of police use of new media and social media technology for public communication. It will take a specific police department, Greater Manchester Police (GMP), as its central case study looking primarily at their use of the popular microblogging service, Twitter and in particular their pioneering use of hashtags. GMP have been praised on both a national and international level for their innovative use of a multitude of different new media technologies and represent an ideal unit of study for the current topic at hand. This chapter will first introduce the historical relationship between the police and technological innovation. The aim of this chapter will be to provide an introduction to the subject of police and social media adoption and use. It will focus on key GMP online strategies in order to provide examples. The preliminary results from a set of semi-structured interviews conducted with GMP officers will also be integrated throughout.

Keywords
Policing, law enforcement, new media, social media services, public sector communication

Introduction

Whilst previous technological developments took some time to reach mass adoption, the internet diffused quicker than any prior equivalent technology. Radio and television took 38 and 13 years respectively to reach audiences of 50 million, whereas the internet had reached a similarly sized group in under four years of its public launch (Qualman 2009), permanently and significantly altering the “landscape of communication and information sharing” (Varano & Sarasin 2014). In the past decade, social media sites have become some of the most visited online spaces. Facebook, currently the most popular of all social media services had reached 1/10 of the world’s population by August 2011 (Varano & Sarasin 2014) and recent statistics from a survey conducted in the US show that 58% of all American adults are now active on the site (Pew 2015). The microblogging service Twitter is now used by 19% of the US adult population with other social
media platforms reaching similar levels of adoption - Instagram 21%, Pinterest 22%, LinkedIn 23% (Pew 2015).

As these online spaces for social interaction have grown in popularity increasing numbers of public sector services have also begun to adopt social media technologies, in order to better communicate with the public they are intended to serve. The internet can now be seen as one of the primary “public gateways into government organizations” (La Porte et al 2002). Yet the response has been far from uniform; public sector services have reacted to this rapid emergence of social media technology in a variety of different ways.

This chapter will examine one arm of the public sector, the institution of the police, beginning with an overall assessment of the field and then moving to a more specific case-study based analysis of a particular UK police force, Greater Manchester Police (GMP), looking at their overall digital output and discussing their adoption and use of the social media service, Twitter. The research reported in this chapter is at an early stage and will aim to further explore the appropriation of various new media technologies by GMP, using semi-structured interviews with a variety of officers and employees. Further ethnographic research based at the GMP headquarters in North Manchester is also planned.

Digital Policing - an overview

A majority of European and North American police departments have now “acknowledged the potential” of the various digital technologies on offer to them and at present are “experimenting with a variety of applications” (Meijer & Thaens 2014). Such ‘experimentation’ will be demonstrated by the case study outlined in this chapter. With regards to the rate at which departments have adjusted to the new media developments, previous research has demonstrated the significant variations with which North American departments adopted the microblogging service, Twitter (Anderson et al 2015). This investigation demonstrated, that at least in the North American case, the response from the police has been varied. Whilst certain departments enthusiastically embraced the potential affordances of social media (with some departments joining Twitter in its earliest days), others have lagged far behind (as can be seen from the few departments which have still not yet joined all of the major social media platforms).

An annual survey conducted by the International Associations of Chiefs of Police in the US provides perhaps the best insight into the current state of new media adoption by police departments. The 2014 survey found that 95% of American police departments now use some form of social media. Facebook (95.4%) and Twitter (66.4%) were by far the two most popular,
with most departments also actively maintaining a website where key information could be found (IACP 2014). A significant number of American police departments began to adopt Twitter as early as March 2009, (Anderson et al 2015).

Within the UK, a similar situation can be observed - a large proportion of UK police departments joined Twitter during late 2008 and early 2009. GMP, the central focus of the case study contained in this chapter, opened their departmental account in February 2009 and at present have close to a quarter of a million followers (233k at the time of writing) on the microblogging service, second only to the London Metropolitan Police (308k). This chapter will return to the details of new media adoption by GMP in more detail but will now move to provide a brief introduction to the historical relationship between the police and technological innovations such as Twitter.

**Police and Technology - a historical perspective**

The tradition of adoption and appropriation of innovative technology such as social media is one that has existed within the institution of the police since its initial inception in 1829, when Robert Peel introduced the world’s first formal police force, the London Metropolitan Police. Facing the problem of “soaring crime rates” Peel and his fellow ‘bobbies’ devised a variety of brilliant yet simple and affordable innovations (Skolnick & Bayley 1986). The adoption of the telegraph by the NYPD, can be seen as one of the earliest identifiable instances of new technologies being embraced by the police before they had reached widespread societal acceptance (Manning 1992). More recently, initiatives such as community policing, Compstat, ‘broken windows’ and evidence-based policing have all been introduced (Braga & Weisburd 2006).

The police have also adopted existing innovations such as the “motorized vehicle, radio communication and computer systems” significantly earlier than other public services. New innovations have found acceptance in certain more innovative police departments long before their use was widespread within society (Varano & Sarasin 2014). With such foundations laid by Peel and his early American counterparts, the enthusiastic approach to innovation and new technology has continued up until the present day. New media, and the various technologies that come with it have helped develop entirely “new models of policing” that are both contemporary yet still firmly rooted in the traditional practices that stretch “through the community policing movement”, right back to Peel’s initial goals “for a modern constabulary” (Davis et al 2014).

In the past thirty years, since the mid-1980s, information technology (IT) has played a central role in the work of police forces worldwide. The adoption of new media (e.g. social media services,
public websites and mobile applications) can be seen therefore as simply a continuation of the ongoing and ever-important relationship between the police and technology.

Previous research has shown that policing is primarily a "technology driven profession" (Varano & Sarasin 2014). Brown and Budney (2003) refer to police officers as ‘knowledge workers’ who are constantly adopting and appropriating the technological tools of the day to their daily operations.

Within the overall institution of policing, innovation can be divided into four individual categories that will be illustrated when discussing the case study in the paragraphs below. These four categories are; programmatic, administrative, technological and strategic (Moore et al 1997). The majority of the examples described below fall into the technological category but some of them, as will be seen, do also have strategic elements to their employment. Within the category of technological innovations further sub-sections have been offered by Byrne and Marx (2011); firstly, ‘information based technologies’ (soft) and secondly, ‘material based technologies’ (hard). The new media technology being discussed in this chapter, such as apps and social media services, can be located at the intersection of these two sub-categories. These initiatives require officers to both be trained in the soft skills of everyday use whilst also being provided with the necessary devices and hardware.

**Technology adoption by the police**

The appropriation of new media by the police can be seen as part of a wider general shift towards open government, one that has emerged in parallel with the rise of the internet. Openness is expected to strengthen the legitimacy of public services in two key ways; transparency and participation (Meijer et al 2012). Evidence of both more transparent and participatory police forces have been displayed by previous research (Mergel 2012, Crump 2011). Persistent use of new media technologies by a department promotes the idea that said department is an organization up to date with contemporary society (Bekkers & Homburg 2007).

The “costs of connecting to citizens” (Meijer 2012) are now lower than they have ever been before, and are continuing to be reduced. Social media services, websites and mobile applications are often very cheap to develop and even cheaper to maintain. A number of the officers consulted as part of the preliminary stages of interviews for this ongoing research project commented that they often use their own personal hardware, such as laptops and smartphones, to maintain their departments online output whether that be through their website or through one of the various social media channels that they offer. In departments where use of personal
devices was completely prohibited the costs were still relatively low, as the cheapest smartphones on the markets can still be more than appropriate for the type of use that most police officers expect of them. This extremely low financial barrier to access and a significant shift in the cost/benefit ratio (Meijer 2012) has encouraged police departments to experiment, with relatively little financial risks associated with failure. It is this culture of open experimentation that can be seen throughout GMP.

Many of the most prominent new media strategies employed by the police have been learnt from the private sector as “businesses have already encountered some of the same challenges” which the police face (Davis et al 2014). However, the police are unique as an institution, and are distinct even “from the rest of the public sector” (Meijer & Thaens 2014) thus they have developed their own models, practices and strategies with regards to the use of new media, some of which will be explored within this chapter.

Communication and conversation have been at the heart of policing practice for many years, but only recently have new media technologies been properly employed to allow this tradition to continue (Davis et al 2014). The communication model for the police and other public services was traditionally structured as a one-way relationship, focused purely on disseminating information to the public (Heverin & Zach 2010). As the new technologies have become part of everyday police work, officers are now more able to talk directly to their communities, which allows for “bi-directional communication” to occur (Varano & Sarasin 2014). Policing, as a discipline, is an “information intensive business” thus any changes in the way society shares information “presents new challenges to the task of policing a democratic society” (DEMOS 2013). New media therefore promises to further strengthen and emphasize the “deep connection” between the police and the communities that they serve (Davis et al 2014). Evidence of such a connection can be seen in the case study included in this chapter. The digitally mediated work of the Greater Manchester Police reinforce the original principle upon which Peel constructed the first police force; namely that the police are the public and the public are the police.

As a significant proportion of police work relies on the maintenance of a trusting relationship with the public how they are perceived by such a public is central to their success. It is undeniable that the police are often entirely dependent upon full cooperation from the public in order “to fulfill their role successfully” (Denef et al 2013). One of the prime examples where police are always in need of input from the citizens that they serve is in appeals to find missing persons (Meijer 2012). Preliminary interviews conducted with UK police officers have found that new media technology, in particular social media services such as Twitter and Facebook, have completely transformed such appeals, as the number of eyes looking for a person can now be
dramatically increased. Such shifts in police practice require more thorough investigation and will form part of the interviews that will follow the research began in this chapter.

The police must protect law abiding members of society, whilst also ensuring the maintenance of rule of law for those who transgress, thus a “continuous balancing act” is always in action (Denef et al 2013). This so-called ‘act’ is equally significant within the online space. The police must be seen to be just and fair, and must maintain their primary community-focused role, whilst also ensuring that those who wish to commit crime online are brought to justice. Yet the potential benefits for police and the online space are huge. New media technologies can offer both support for investigations (primarily through an ever-increasing potential corpus of intelligence) and, more centrally to the focus of this chapter, an ever more “direct path of communication with the public” (Denef et al 2013). Aside from these two central facilities of new media there is also huge potential for digital assistance in tackling crisis situations, controlling crowds and advertising to potential new recruits (Meijer & Thaens 2014). An examination of the various new media output channels of the department studied in this chapter, GMP, provides evidence for all of the above tactics.

The aforementioned IACP survey provides further insight into the various reasons why certain police departments have so enthusiastically employed new media technologies and what exactly they are using the various services for. Over 80% of departments surveyed said that they regularly used new media, and in particular social media tools for criminal investigations (IACP 2014). The next two most popular uses of the technology, however were for notifying the public of key issues in the community (78.9%) and improving community outreach and citizen engagement (77.8%). It is questions such as this which the research project that this chapter will form a part of, will aim to address. In recent correspondence with one of the foremost researchers in this emerging discipline of police and new media, Sebastian Denef, he commented that many of the US police officers he has encountered refer to themselves as law enforcement first and foremost (Denef 2015). Meanwhile, police officers across Europe, and in particular within the UK and the Netherlands, rather see themselves as primarily community officers (COMPOSITE 2013).

There are of course obstacles to the adoption of new media by the police. One of the primary examples of such an obstacle are the “extensive legal frameworks that bind police behavior” (Denef et al 2013). In a number of the preliminary off-record interviews conducted as part of this research project a number of the officers consulted said that their superiors had repeatedly expressed fear at causing legal problems for themselves in the future if they embraced certain new media technology, such as the microblogging service Twitter, without proper assessment and foresight. Police departments are constantly treading a fine line between keeping up to date with technological developments, whilst also maintaining proper practices and ensuring that the
rule of law is maintained. Aside from the most prominent legal issues the use of new media by the police also poses the threat of a PR disaster that can be seen by all. Misuse of the internet and its related technologies can, and in the past has, opened the police up to “scrutiny and comment by the general public” (Denef et al 2013).

The case study outlined in this chapter, that of Greater Manchester Police, illustrates the police adoption of social media and highlights some of their most significant successes. The four strategies outlined in the below discussion are all evidence of this mindset that approaches new technology with open arms rather than fear and hesitation, and accepts that PR disasters will always be a potential yet avoidable risk.

**Case Study - Greater Manchester Police**

The Greater Manchester Police force (GMP) serves an incredibly diverse (both economically and ethnically) area of just under 500 square miles, with a population of just over 2.5 million. It has just under 7000 active constables and is one of the oldest police forces in the UK, having been established shortly after the inception of the London Metropolitan Police Service. They have received praise for their wholehearted embrace of the online space, and in particular their enthusiastic use of social media. In recent years, along with most of the police forces in the UK, the GMP has experienced significant cuts in their budget. Department estimations suggest that the force lost close to 300 frontline officers during last years round of cuts and are expected to lose many more in the coming years. In this uncertain financial atmosphere GMP have been forced to look for methods of communication with the lowest cost barriers. Preliminary interviews have suggested that whilst money was not a central consideration in terms of their decision to adopt social media so significantly, it did indeed play a role.

The current case study will outline some of the key online outputs of the force. The GMP website and app will be discussed, before then moving to a more in depth analysis of their use of the microblogging service Twitter, with a particular focus on their pioneering use of hashtags (many of which were then taken on by other police departments across the UK and abroad). Key initiatives such as #westandtogether, #gmp24 and #itsnotokay began life within GMP and have now been adopted and imitated by a number of other police departments, both in the UK and further afar. Such initiatives perfectly encapsulate both the passion and professionalism with which the GMP and its officers have approached the online space as a whole.
GMP Website - www.gmp.police.uk

Police websites provide a place where an “unlimited amount of information” can be disseminated to “citizens in a structured manner” (Meijer 2012). Previous research has demonstrated that they are also a key site for identity construction for all manner of organizations, police or otherwise - via their online presence police departments can create multiple identities, and through such multiplicity can provide support for “claims for legitimacy” (Sillince & Brown 2009). Police websites can be seen as a “window into the psyche” of police departments, specifically in terms of how they view their relationship with the public they are intended to serve (Rosenbaum et al 2011). Department websites have “the potential to answer public demands” yet, as is the case with all of the technologies discussed in this chapter whether “agencies take advantage of this opportunity” is another matter (Rosenbaum et al 2011). Research into the use of websites by the police has been carried out in locations as diverse as the Netherlands (Korteland & Bekkers 2007), India (Mitra & Gupta 2007) and the US (Rosenbaum et al 2011).

Greater Manchester Police are a prime example of an organization that understands the value of maintaining a positive identity online and view their website as a potential primary site of image construction. They were one of the earliest police forces to have an actively maintained website in the UK and their website has undergone a number of redesigns over the years, often proving popular with both local media and the wider general public.

The most recent update of the website received its launch at the beginning of April this year. It was the result of a number of feedback sessions with the general public in Manchester and now includes an ‘add my community’ function which allows the public to “personalize the information they receive depending on where they live or work in Greater Manchester” (Manchester Gazette 2015). The website has also been updated to be more suitable for smartphone and tablet users, which make up an ever-increasing section of the online crowd. In an interview with a local newspaper DCC Ian Hopkins, one of the primary leads for new media development at GMP, expressed his excitement at the new and improved site, and gave an insight into the process of its development; “we have listened to feedback from the public on how we can improve the website and tried to put that into action…I hope the new features and layout will keep the line of communication between the public and police wide open” (Manchester Gazette 2015). This sentiment further echoes the earlier discussed Peelian principles upon which all police departments base their practice.
The GMP site also contains a missing persons section, a most wanted list and an area where potential new recruits can browse any current vacancies. There is also significant integration with the various other new media channels of the GMP, some of which are discussed in more detail below. The social media channels are embedded along the side of the page and in the most prominent position at the head of the homepage is a link to download the recently revamped GMP mobile application. The website is maintained and updated regularly. It can be seen as the start page from which a member of the public can access the rest of the various new media channels on offer from the GMP. An additional section contains a blog from the current GMP Chief, Sir Ian Fahy, which is yet further evidence that the entirety of the department, from top to bottom, fully recognizes the potential of the online space for the practice of police-public communication.

**GMP Mobile Application**

GMP were the first police department in the UK, and one of the first in the world, to develop their own free-to-use mobile application. Similar to their website, whilst the first version was
launched just over two years ago at the start of 2013, it has since received a number of redesigns and additions and is now available on all smartphone devices, both iOS and Android. The app utilizes “geolocation technology” to allow the Manchester public to “contact the force directly” and also have easy and location specific access to “police information” (ITV News 2013).

As well as the initial canvassing of the public in the first stage development of the app, DCC Ian Hopkins encouraged people to suggest additions and updates that they themselves would find useful on a day-to-day basis, commenting “we want people to help us” (GMP Website 2013). The app has proved popular with the Manchester public and has been downloaded by many thousands of different users. It is further evidence of GMP’s recognition that the police should always concern themselves with involving the public as much as possible, and that new media technology is perfectly suited to encourage this all-around beneficial codependent relationship. The only potential downfall of the mobile application is that it is not very well known about due to a lack of advertising, and thus far its reach has been relatively limited, at least in terms of the overall online population of Manchester. This should not detract from the fact that GMP took the first step amongst UK and European police forces to move into the app market, and have actively included both positive and negative suggestions in each redesign, a move worthy of significant praise.

**Watershed moment - GMP use of Twitter during the 2011 UK Riots**

On 4 August 2011, a young man from Tottenham, Mark Duggan, was shot dead by a London Metropolitan Police Armed Response Team, as he travelled in a taxi through London. Questions about whether the police officers in question acted within the confines of the law and in self defence led a group of locals, fronted by Duggan’s family, to the local police station to demand
answers. When no answers were given unrest slowly turned into a full scale riot within 48 hours of the original incident. Over the days that followed the riots spread from North London to other Metropolitan boroughs, before then moving to other major UK cities, including Liverpool, Birmingham and Manchester (Denef et al 2013).

New media technologies played a significant role in the ensuing chaos. A large section of the rioters used services such as Blackberry Messenger (BBM), a once popular instant messaging service, to coordinate their activities and at one point there were calls by the UK Prime Minister, David Cameron, to turn off the network altogether (BBC News 2011), which were eventually dismissed. During the peak of the unrest and equally in the immediate aftermath a number of UK police departments, many of which had only recently adopted social media services into their everyday practice, began to use platforms such as Flickr, Facebook and primarily Twitter to at first contain the situation and then subsequently begin the process of bringing those responsible to justice. The role of social media within the riots has thus been the subject of a significant amount of academic research and investigation (Denef et al 2013, Baker 2012, Procter et al 2013, Tonkin et al 2012).

Denef et al (2013) examined the role of social media in the riots from a primarily police-oriented perspective. They compared the use of the microblogging service Twitter by the two largest police departments active in the UK, the London MET and GMP. Their primary finding showed that the MET preferred to maintain a certain distance from the public, employing an instrumental approach where the primary role of new media technology was as a place from which to disseminate warnings and statements to the rioters and the general public. In complete contrast, GMP employed an expressive approach and were more open to criticism and maintained a direct line of two-way communication with the online crowd.
GMP’s open embrace garnered not only academic investigation but also significant media attention (Mashable 2011, MarySue 2011, The Next Web 2011). Whilst some of this media attention was raising potential conflicts that could arise in the future from such an open and transparent approach to the criminal justice system, on the whole GMP were praised for being willing to divert from the usual practices of policing, many of which are not up to date with the current developments in new media. The New Scientist (2013) followed up the article from Denef et al (2013) with interviews with two of its authors, both of whom praised the actions of GMP, whilst admitting that at the time it was seen by many to be controversial.

**GMP use of Hashtags**

#GMP24

![Fig. 4: Tweet from the 2010 edition of GMP24](image)

GMP24 was an initiative launched in 2010, soon after GMP first adopted Twitter as one of their primary sites for public communication. It was considered a success and has since been imitated by a number of other police departments, in the UK and further abroad and was subsequently repeated last year. It has since received praise from both local (MEN 2014) and national (BBC 2014) media.

![Fig. 5: Screenshots of GMP tweets concerning the GMP24 initiative](image)
The concept behind the hashtag was to tweet everything that the GMP received calls and attended to during a 24 hour period, only withholding information that could be considered too private or even too case-sensitive. During the second run of the initiative, in 2014, GMP received a total of 2,626 emergency calls during the fixed 24-hour period. The general aim of the initiative was to give the Manchester public a better insight into the types of incidents that the police are called to deal with.

#WeStandTogether

![Image](image.png)

Fig. 6: The primary banner for the westandtogether initiative

In the immediate aftermath of the Charlie Hebdo attacks in Paris and the terrorist incidents in Copenhagen questions were asked of the successes and failures of minority ethnic community integration across major European cities. As a direct response to this the Chief of GMP Sir Ian Fahy launched the #westandtogether initiative with the direct aim of reaching out to Muslim community leaders across the Greater Manchester Area.

![Image](image.png)

Fig. 7: Tweets from one of the recent westandtogether events in Greater Manchester

The initiative began in March of this year and was introduced by a 5 minute video that featured interviews with a variety of well-known individuals from the Manchester area, all of whom were promoting better integration and community involvement within the city. The initiative aims to bring people “together as one to celebrate their differences in order to build a safer and stronger”
environment in which to live (GMP 2015). Chief Fahy insisted that #westandtogether would help send a “strong unified message that any attempt to create disharmony or fear is futile” (GMP 2015). The primary UK national policing body, the ACPO, saw so much merit in the initiative that they decided to roll it out nationwide, yet another example of a GMP social media communication strategy that garnered them both national and international praise. Other UK police forces, such as the City of London, South Yorkshire and Merseyside (three areas with large Muslim populations) have actively supported the initiative and have mirrored the GMP approach of using online tools to advertise real world meetings where community leaders from all ethnic and religious backgrounds can meet to discuss and move together towards better urban integration.

#ItsNotOkay

Fig. 8. The homepage banner of the ItsNotOkay central website

The #itsnotokay initiative focused on tackling child sexual exploitation in the Greater Manchester area. It represents a collaboration, led by the GMP, of various public and third sector organizations within Greater Manchester. The list of partners is extensive and features various police agencies, national health bodies and local council figures as well as various related charities (ItsNotOkay 2015). It is the first partnership of its kind within the UK and has employed Twitter as one of its primary mediums for public communication.

Fig: 9: Tweet concerning the launch of the ItsNotOkay citywide initiative

GMP officers have since set up a separate Twitter account for the itsnotokay campaign, which now has more than 1,000 followers. Once more, the initiative since been emulated and imitated by other police forces across the UK, further testament to the impressive record the GMP has with using social media technology for communication with the public. It is this impressive record that shall be the focus of continued investigative research over the coming year.
Preliminary results and future research

As part of the ongoing research project of which this chapter will form one part a series of interviews have been conducted with officers from the GMP. The key strategies outlined above have been discussed in all of the interviews and the preliminary results can be introduced here. One of the main comments that kept being made was the significant community impact that the GMPs use of Twitter has had thus far. One officer, from a particularly diverse area of Greater Manchester, commented that he had figures from both the Muslim and Jewish community following him on Twitter and thus he was able to build relationships online that could then be solidified at community meetings and town hall events.

The same officer commented that whilst Twitter and other services such as the website are very useful they “are just one part of the way we communicate with the local community”. All of the officers interviewed stressed that social media should not be seen as a magic solution to the ever-changing demands of modern policing. Rather, it should be seen as yet another valuable tool that the police can employ in order to better communicate and build relationships with their public.

Another common theme in the preliminary interview round was the far reaching potential of social media to inform the public about the diversity of present day police work. The GMP24 initiative was raised by all of the officers, and all reflected that it was one of the biggest successes of the past 5 years of GMP online output. One officer commented that in the past they had to rely on the press in order to educate the public about their daily work, whereas now “we can do it directly”. Added to this one officer commented that he had had people approach him whilst out on the street and comment that they had never been aware of the huge variety within policing before they read the information being tweeted on one of the GMP24 Twitter days.

One of the primary areas for further investigation will be uncovering the primary drivers of social media adoption and subsequent use within GMP. One of the officers interviewed commented that the westandtogether initiative was the brainchild of the Chief of GMP, and then was taken on by other staff members until it received nationwide attention. Another key figure of the GMP online output, the head of corporate communications, was praised by a number of the officers interviewed, for taking on her own initiative and driving social media activity relentlessly both as an individual and as a member of the GMP staff.

In one interview an officer commented that he had observed some individuals “who were really proactive and really enthusiastic” whilst there were many others, often the older members of
the force “who really aren’t interested at all” in the potential affordances of social media technology. Such insights raise questions about what matters most in terms of police use of social media - is it the individuals within or the overall organization itself which factors most. The likely answer is that it’s a combination of the two, yet this is certainly a subject that warrants further questioning.

This chapter has provided an introduction into police use of internet-based technology for public communication. It began with a summary of the historical relationship between the police and innovations in technology, before moving to look at more recent studies of the police using social media. In the final section the online activity of the Greater Manchester Police was examined in some detail and preliminary interview data was included to support the key claims made. The research began in this chapter will continue with another series of semi-structured interviews. Added to this, interviews are currently being scheduled with one other UK police department which will be enable a comparative study to be carried out.

References


Baker, S.A. 2012. From the criminal crowd to the “mediated crowd”: the impact of social media on the 2011 English riots. Safer Communities, 11:1, 40 – 49.


Varano S.P & Sarasin, R. 2008. Use of Social Media in Policing School of Justice Studies, Roger Williams University, Bristol, RI, USA

WEB LINKS

http://www.pewinternet.org/2015/01/09/demographics-of-key-social-networking-platforms-2/
http://manchestergazette.co.uk/30371/greater-manchester-police-launch-new-website
http://www.themarysue.com/uk-police-social-media/
http://searchenginewatch.com/article/2066771/Social-Media-Fad-or-Revolution
http://www.itsnotokay.co.uk/who-we-are/