Future Internet **2013**, *5*, 205-236; doi:10.3390/fi5020205

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Review

A Review of Cyber Threats and Defence Approaches in Emergency Management

George Loukas *, Diane Gan and Tuan Vuong

School of Computing and Mathematical Sciences, University of Greenwich, Old Royal Naval College, SE10 9LS, London, UK; E-Mails: d.gan@greenwich.ac.uk (D.G.); t.p.vuong@greenwich.ac.uk (T.V.)

* Author to whom correspondence should be addressed; E-Mail: g.loukas@gre.ac.uk; Tel.: +44-20-8331-9612.

Received: 17 February 2013; in revised form: 19 March 2013 / Accepted: 10 April 2013 / Published: 7 May 2013

Abstract: Emergency planners, first responders and relief workers increasingly rely on computational and communication systems that support all aspects of emergency management, from mitigation and preparedness to response and recovery. Failure of these systems, whether accidental or because of malicious action, can have severe implications for emergency management. Accidental failures have been extensively documented in the past and significant effort has been put into the development and introduction of more resilient technologies. At the same time researchers have been raising concerns about the potential of cyber attacks to cause physical disasters or to maximise the impact of one by intentionally impeding the work of the emergency services. Here, we provide a review of current research on the cyber threats to communication, sensing, information management and vehicular technologies used in emergency management. We emphasise on open issues for research, which are the cyber threats that have the potential to affect emergency management severely and for which solutions have not yet been proposed in the literature.

Keywords: survey; pervasive computing; network-level security and protection; physical security; emergency management

1. Introduction

Emergency management (EM) increasingly depends on computational and communication systems for coordination, communication, information gathering, training and planning. For example, wireless

sensor networks can contribute towards early detection of emergency events [1,2], as well as improved situational awareness during a search and rescue operation, at the level of individual buildings [3] or larger geographical areas [4]. Autonomous systems and particularly autonomous vehicles are also commonly proposed in the EM context. Situational awareness and coordination may be improved with live aerial imagery provided by unmanned aerial vehicles [5] or with an ad hoc infrastructure of wireless robots that reach locations otherwise inaccessible to the first responders [6]. The Internet also plays a significant role, with several web-based EM systems, as well as with the widespread use of social media for the dissemination of information during an emergency, both by the authorities and the public [7,8].

This increased use of computational and communication systems introduces cyber threats in EM. Cyber attacks can directly cause physical damage or indirectly aggravate a physical incident by impeding the work of first responders. As EM makes use of several private and public communication systems, from satellite communications to wireless sensor networks, cellular networks and the Internet, a security breach in one communication medium can have an impact on all other ones. In fact, the prevalent use of cyber-physical systems means that a cyber attack can even affect the operation of physical devices, such as flood control equipment or safety sensors. At the same time, decisions during an emergency need to be taken and communicated quickly. A cyber attack that would target the integrity of the information could have an immediate effect on the decision making that relies on that information, while a denial of service attack could cut off communication between commanders and first responders. The various EM interdependencies have been categorised by Dudenhoeffer *et al*. into physical, informational, geospatial, policy/procedural and societal ones [9,10].

Our aim is to illustrate the landscape of the EM-related information security research and identify areas of priority where further work is needed. We have previously discussed the security threats to EM networks and their unique challenges in terms of time-criticality, system interdependencies and the human element [11]. Here, we attempt to cover the broader spectrum of computational and communication threats in relation to the technologies used in the mitigation, preparedness, response and recovery phases. The four phases comprise what is known in EM as the *Comprehensive approach*, originally proposed in 1978 and, although challenged over the years [12], still in use in the United States, the UK and Commonwealth, and several other countries. By following the widely used *Comprehensive approach* terminology, our aim is to facilitate communication between information security and EM practitioners and researchers.

1.1. Mitigation

Mitigation refers to actions taken to decrease the likelihood that an emergency will occur and reduce its impact should it occur. Geographical Information Systems (GIS) are often used to identify geographical areas of high risk that would need to be prioritised during an emergency, and disaster databases are used for research and risk analysis, informing policy making and emergency planning.

1.2. Preparedness

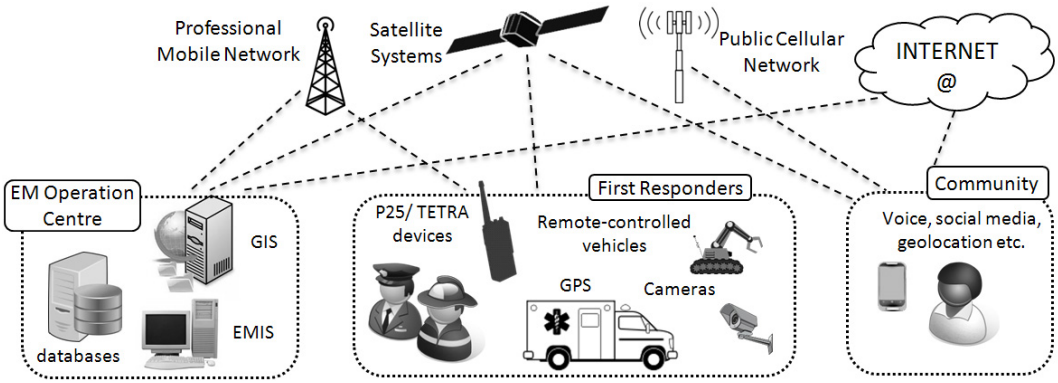
Preparedness refers to the development of policies and protocols, incident command systems, training, planning, coordination, and public awareness for potential emergencies. Simulation software may be

used for analysis and training [13,14], while disaster databases and GIS systems may help identify evacuation routes, shelters and relevant resources [15].

1.3. Response

Response actions aim to effectively contain and resolve an emergency after it has occurred. They often involve the mobilisation of multiple emergency services, such as fire-fighters, the police, ambulances and specialist rescue teams, as well as the participation of volunteers. The operation carried out relies on EM plans and processes defined in the mitigation phase and rehearsed in the preparedness phase. During emergency response, a wide range of technologies are used. The Internet and social media may be used to report casualties and damage and to communicate with volunteers, while space technologies may be used for asset tracking or to establish communication where terrestrial systems have failed. Professional mobile radio is typically used between EM practitioners, while a number of vehicles and devices of varying sophistication may be used to spot, communicate with or transport those affected (Figure 1).

Figure 1. Example of technologies involved in the Response phase.



1.4. Recovery

The process of assisting the affected community and restoring the infrastructure often relies on the existing EM organisational systems and processes. GIS systems and geospatial databases can be used not only to plan aid and reconstruction, but also to monitor these processes [15]. Recovery may also involve disaster medicine, which in turn depends on a networked infrastructure for health-related information gathering and for early warning of authorities and the public. Healthcare in general depends on computerised equipment, which can be disabled by common web-borne malware, as in the case of Sweden's MRI machines and heart monitors in 2009 [16]. Harries and Yellowlees have recently presented evidence that the risk of cyber-terrorism targeting the US healthcare system is increasing and have provided best practice suggestions that can be adopted by healthcare organisations [17].

2. Overview of Cyber Threats in EM

During an emergency, human mistakes are naturally common. Time pressure and the lack of familiarisation of EM practitioners with concepts of cyber security [18] would make it relatively easy

for cyber attackers to exploit human mistakes, possibly through social engineering. The insider threat or Man-at-the-end attack, as suggested in [19], may also be significant. For example, in 1992, a failure of Chevron's computerised emergency alert system delayed the authorities from notifying the public of a chemical release accident. The failure was caused by a disgruntled former employee who had disabled the emergency alert function [20]. While the human element is certainly critical in the EM context, our emphasis here is on the vulnerabilities of the technologies involved (Tables 1–3).

Table 1. Communication security threats and proposed EM countermeasures.

Technology	Security threat	Impact	Countermeasures
SMS Messaging	Weak message authentication [21]	Rogue messages transmitted	Adoption of CB [21]
	SMS Flood [21]	Voice network overload, messages lost/delayed/out of order	Adoption of CB [21]
Cell Broadcast (CB)	Weak message authentication [21]	Rogue messages transmitted	Encryption [22,23]
	Control channel jamming [24,25]	Loss of availability	Antijamming mechanisms [24,26]
Amateur Radio	Fake GSM and other stations [27]	Calls spoofed/intercepted	No known solutions
Professional Mobile Radio	TETRA authentication key cloning [28]	TETRA authentication process compromised	No known solutions
	Radio location privacy attack [29]	P25 Location privacy breached	No known solutions
	Physical layer jamming [29]	P25 Denial of service	No known solutions
	Brute Force Key recovery [30]	P25 authentication process compromised	No known solutions
Satellite Communications	Weak satellite phone encryption [31]	Interception of calls	No known solutions
Satellite Communications	Excessive traffic through satellite link [32]	Loss of availability	Egress filtering at connected networks [32]
Wireless Communication Networks	Rogue nodes [33,34]	Unauthorised use	Pre-shared keys [33,35] list of approved devices [36], IDS [37], RFID [38], Hardware Security [39]
	Eavesdropping [33]	Breach of confidentiality	IPSec tunnel [33]
	Poor physical security [40]	Access to crypto credentials/Insider threat	Message-based content verification [41]
	Availability attacks (DoS, Jellyfish, grayhole, blackhole *etc.*) [40,42]	Loss of availability	Redundancy, traffic shaping and IDS [43], Oppcomms [44]
World Wide Web	Web-based attacks [45,46]	EM websites and web-based information systems affected	Web Security literature [46]

Table 1. *Cont.*

Technology	Security threat	Impact	Countermeasures
Social Media	Account hijacking/relay attack [47]	Rogue messages transmitted on behalf of emergency services	Social media management applications
	Intentionally false information provided to emergency services [47]	EM influenced by misleading information	No known technical solutions. Discussion provided in [48]
	Bot-generated messages [47]	Spam or misleading information sent to EM Social media account	Random Forest Classifier for bot detection [49]

Table 2. Sensing security threats and proposed EM countermeasures.

Technology	Security threat	Impact	Countermeasures
Satellite-based Sensing	GPS Spoofing [50]	Misleading GPS coordinates used for positioning calculations	Signal analysis [51–53]
	On-board computer reconfiguration [54]	Covert activity	No known solutions
	Jamming	Loss of signal	Multiplexing, Spread-Spectrum, EHF frequencies, directional antenna beams, signal processing *etc.* [55]
Sensor Networks	Compromised node [56,57]	Battery exhaustion, spoofed/altered/replay messages	Detection based on both network and sensor measurements [58], collaborative sensor detection [44,56,57]
	Sybil attack [59]	Multiple fake identities used to collaboratively overcome cryptographic techniques	Collaborative detection [60]
	Rogue nodes in EM medical body sensor network [61]	Unauthorised use	Light-weight cryptography [62]
	Denial of service in EM medical body sensor network	Loss of availability	Body sensor network IDS [63]

Table 3. EMIS security threats and proposed countermeasures.

Technology	Security threat	Impact	Countermeasures
EMIS	Attack on satellite sensing	Inaccurate mapping	Satellite sensing countermeasures (Table 2)
	SQL injection and other database attacks [64,65]	Inaccurate database information, breach of data confidentiality	Database protection measures
	VoIP attacks [66,67]	Eavesdropping, spoofing, masquerading *etc*.	VoIP security literature [66,68]
	Weak authentication	Unauthorised use, breach of privacy	Role based Access Control [69], document encryption [70]

Likewise, the protection of EM against cyber threats can be enhanced through strengthening the technology, the processes or the awareness of people involved. Each EM-supporting system may need to be updated and patched regularly to avoid attacks on known vulnerabilities, as well as to keep appropriate logs for detecting and investigating cyber events. Process practices and guidelines would bring the level of security of Emergency Management Information Systems (EMIS) up to date with industrial standards and would assist auditing. Human mistakes and susceptibility to social engineering could be reduced through training programs for EM personnel, as well as through the introduction of strong cyber security policies on user privileges. Such procedural improvements to information security have been discussed in [18] and a prime example is the Red Cross, whose engineers maintain ghost master system images with operating systems and software needed in disaster zones. They keep them patched and updated, so that when needed, they can load them on the laptops and deploy them fully patched before first use, thus saving time and protecting their mission from common cyber threats [32]. Nevertheless, our focus below is on technological improvements rather than procedural ones.

2.1. Communication Media

EM organisations are becoming increasingly aware that a terrorist attack may target key communication infrastructure to maximise the impact of a simultaneous physical attack. The potential impact of malicious communication disruptions has been demonstrated over many recent high-profile disasters where emergency response was hampered by a failure of the communication infrastructure, because of network overload, as in the 9/11 attacks, or because of physical damage, as in Hurricane Katrina and the Haiti earthquake. Lack of reliable communications may result in greater loss of life, as rescuers cannot coordinate effectively and the public is not warned in a timely manner. In [71], Walker has suggested that the EM community would most likely be incapable of an effective response to a terrorist attack on a major metropolitan area if a cyber attack had previously crippled the communication and data networks on which EM relies. However, it is not only the availability of communications that needs to be maintained. Attacks targeting the integrity or the confidentiality of information transmitted could also affect the effectiveness of EM. As a result, it is rather worrying when new protocols currently developed for emergency service communication, such as 802.23, include no special measures for security. Here we discuss what we perceive as the main security threats to currently used

EM communication technologies. We discuss both defence mechanisms that are already in use or have been proposed and open issues for security research that, to date and to the best of our knowledge, have not been addressed yet.

2.1.1. SMS Text Messaging

SMS Text messaging is often used by the authorities and third parties to rapidly disseminate critical information during emergencies. For example, after the 2004 Indian Ocean Tsunami, a number of SMS-based tsunami warning systems were developed and introduced in South East Asia [15]. However, recent research has shown that these messages could overload the cellular network and cause failures during the emergency that were previously not understood [72]. There is clearly no malicious intent behind emergency text messaging, but it has demonstrated the vulnerability of the cellular network to simple SMS flooding attacks during an emergency.

SMS messages are not encrypted by default, but the SMS standard does provide optional mechanisms, such as redundancy check, cryptographic checksum and digital signature to verify confidentiality and integrity of data. Each message has a specified validity period after which it is deleted by the network provider.

Open issues in security of SMS Text Messaging used in EM: Traynor *et al*. [72,73] have provided a mathematical analysis showing that mobile voice service in a city the size of Washington D.C. can be denied completely with little more than a cable modem generating 240 messages per second. Such rates can be achieved by using External Short Message Entities (ESMEs), including web-based messaging portals at service providers' websites and software applications. As countermeasures, they have recommended the separation of voice and data traffic, strict resource provisioning, direct channel allocation, rate limitation and particular ESME security measures, but a cyber criminal can still overwhelm the network by using a large enough botnet. The same authors' simulation results in [21], on the use of emergency text services in university campuses and backed by historical data, have shown that only 20% of students would receive these messages in a timely manner. The rest would never receive them or would receive them with over five hours of delay. As SMS services are usually configured to retransmit a message automatically, dropped messages increase the load on the network, further disrupting voice communication. Finally, when multiple messages are sent over the course of the same emergency, the loss and delay of messages, as well as the use of different queuing algorithms by different service providers, may cause messages to be received out of order or out of context. A number of examples of real emergencies where confusion was further increased due to out of order emergency text messages have been provided in [21]. Thus, defence against bot-generated SMS floods during an emergency is a significant open issue.

2.1.2. Cell Broadcast (CB)

CB has been developed as part of the GSM standard. It is used for one-to-many messaging to specified mobile network cells as an alternative to the one-to-one SMS messaging. It utilises the existing mobile telecommunication infrastructure, but unlike SMS, it is not affected by traffic overload. In Japan and Korea, CB has been used for several years for public warning and communication between

relief workers. Since 2005, European mobile network operators have started deploying the capability to transmit government text warnings via CB, and most recent mobile devices are CB-enabled.

An initial approach for authentication of CB messages was provided in [22], where mobile stations' access to a cell broadcast message is limited through encryption before transmission. A more recent authentication mechanism that differentiates between logical broadcast channels has been presented in [23]. It specifies that a message control node receives the initiation request identifying a first message payload segment to be transmitted, determines the authentication group for which it is intended and a first encryption key associated with the authentication group. These mechanisms have been designed to reduce the likelihood of rogue messages being transmitted over CB, but would provide only limited protection against availability attacks.

Open issues in security of CB used in EM: Considering that CB was introduced partly to address the bandwidth issues of SMS messaging during emergencies, it is significant to note that it does not include any provisions for addressing localised denial of service attacks, such as the ones that can be generated by cheap close proximity jammers. If the data and control message channels can be identified, then a control jamming attack can be launched, using significantly lower energy than what would be required to jam all communications channels [24]. If the attackers are already in the network, as insiders or following a successful masquerading attack, a technique detailed in [25] can be used to prevent mobile stations from communicating. It involves jamming only one in 51 frames on a control channel. Recently, Liu *et al*. [26] have proposed a randomised distributed scheme that allows nodes to establish and maintain the control channel in the presence of an insider acting as a jammer, even if the latter has knowledge of the protocol specifics and of the cryptographic quantities used. Their approach, however, assumes that there is a sufficient number of participating nodes in order to be able to cooperatively identify the compromised ones. In an emergency situation where a large part of the infrastructure has been destroyed, this may not be the case. Defence against localised jamming of the CB channels during an emergency, especially from an insider, is an open issue for research.

2.1.3. Amateur Radio

During the Sichuan earthquake in 2008, trained amateur radio operators set up personal radio stations to establish emergency communications, using authorised frequency bands. The local response coordination depended entirely on this network because all other communications had been lost [15]. Amateur radio is a very common solution during a disaster.

In the past, the security of amateur radio was not a great concern due to the limited range and high cost of the equipment, but this is gradually changing as software defined radio (SDR) has introduced new security threats into the mobile communications of emergency services. Up to now, there has been practically no security measure in place for preventing a malicious user from launching SDR-based attacks against wireless communications.

Open issues in security of Amateur Radio used in EM: As specified in [27], a SDR attacker requires only a PC, a front end to capture traffic, a high-speed Analogue-to-Digital Converter (ADC) to digitise the radio frequency signal, and a Digital Signal Processor (DSP) for analysing it before converting it into audio. The user then analyses the spectrum looking for repeating patterns to isolate the preamble and payload or the message header. Frequency hopping and advanced modulation techniques can be

overcome by SDR. Most significantly, SDR is not restricted by frequency. This means that it can provide the means to compromise GSM, WiMax and other wireless communication technologies without expensive dedicated hardware. It has been estimated in [27] that a fake mobile base station can be created with approximately £500. This would provide a criminal with all the tools required to capture a signal, modify and re-broadcast it, create fake GSM base stations, and even send altered signals to roadside matrix boards. Currently, SDR attacks are particularly difficult to prevent. It would require the targeted wireless system to have been designed with particular provisions in place for preventing over-the-air attacks.

2.1.4. Professional Mobile Radio

Communication between EM personnel, vehicles and equipment is often based on domain-specific mobile radio technologies, such as Terrestrial Trunked Radio (TETRA) developed in Europe and P25 developed in the United States. TETRA and P25 networks do not suffer the congestion issues of public cellular networks, but provide low communication speeds in comparison with modern standards.

TETRA and P25 have been designed with protection against eavesdropping as a primary consideration from the start. TETRA relies mainly on four encryption algorithms (TEA1-4), which differ depending on the organisation involved (commercial *vs.* public safety; and whether within the EU or not). It supports the mutual authentication of a mobile station and the network, so as to control access to the network and for the mobile station to check whether the network can be trusted. Keys can be static or dynamic depending on the situation, terminals can be disabled if lost or stolen, and encryption is end-to-end. As one would expect, details of the implementation of each encryption algorithm in P25 and TETRA have not been published, but their security architectures have been detailed in several publications [28,29].

Open issues in the security of Professional Mobile Radio used in EM: Despite the emphasis of TETRA and P25 on relatively strong encryption approaches, researchers have identified flaws in both. TETRA's TEA2 advanced cipher, which is available only to European public safety organisations, has been shown to be unable to protect against attacks that clone both the terminal identifier and the authentication key if the latter were exposed when distributed to the authentication centre [28].

One of the first known security analyses of P25 has been published in [29]. Its authors have used the GNUradio open-source SDR software as their research platform and have identified that the lack of authentication on P25 voice and most other types of data traffic constitutes a significant problem. They have demonstrated a location privacy attack that can locate a radio even when its user is not actively using it. They have also discussed a physical layer jamming technique that can be used to perform denial of service. As communication speeds provided by P25 are already relatively low, a denial of service attack would have a severe effect on the first responders' coordination during an emergency.

Also using GNUradio as the basis of their investigation, Glass *et al.* [30] have developed an open-source P25 packet sniffer and analyser. With this system in place, they have demonstrated how to bypass the authentication and access control mechanism and how to disable specific nodes at will, as well as passive recovery of encryption keys. In a laboratory environment, they have captured traffic from various radio systems and transmitted and received them using P25 radios. Most significantly, they have described in detail a widely-used proprietary P25 cipher system and have shown how to recover the encryption key without considerable effort. According to their research, this is primarily the result of the

fact that encryption is optional in P25, thus allowing a malicious user to inject messages in the clear that the network infrastructure will handle as if they are legitimate. Another significant shortcoming is the lack of a key hierarchy, which means that a single key is used to encrypt traffic between many users over many sessions.

As the authentication of both TETRA and P25 has been shown to be possible to overcome with only low cost equipment, it is not safe to assume that passive cryptographic mechanisms will be enough to protect communication over professional mobile radio during an emergency. Thus, an open issue for research is the development of active methods for detecting a successful security breach.

2.1.5. Satellite Communications

Satellite radio [74], hybrid terrestrial-satellite mobile networks [75] and other satellite network systems have been proposed and some are routinely used for disaster recovery [76]. An example such system that combines satellite and mobile phone technologies is used in South Africa as an emergency alert system [15]. CISCO's hastily-formed network (HFN) approach for emergency response and disaster relief also relies heavily on satellite Internet when the terrestrial infrastructure is degraded or destroyed. While costly and slow, it can be rapidly deployed and may be the only available option in a disaster environment [77]. Common types of portable satellite systems are VSAT (Very Small Aperture Terminal) and BGAN (Broadband Global Area Network). They need to have clear line of sight to the provider's satellites and provide speeds from 128 kbps to 30 Mbps, but typically at the lower end [32,77].

Satellite communication is generally unreliable. Service can be temporarily degraded due to too many terminals in one area or due to a storm over the end-user's ground terminal or the provider's earth station [77]. Although not strictly a security measure, quality of service algorithms can prove useful by compensating for the high latency and jitter experienced by satellite voice and video communication end-users [77].

The availability of satellite communication has traditionally been a significant concern, especially in the defence sector. For this reason, several anti-jamming technologies have been employed on military satellites. These may include Spread Spectrum, EHF frequencies, directional antenna beams and signal processing techniques for jamming mitigation, which are typically not used by commercial satellites [55] employed in EM. As the technologies exist though, this is related to commercial decisions rather than a technical research issue. However, satellite communication availability can also be disrupted via cyber means, such as a network denial of service attack. We describe the related open issue for research next.

Open issues in security of Satellite Communications used in EM: Due to its low capacity and its role as the Internet gateway at locations where there is no other direct Internet access, the satellite link is often a bottleneck on which local wireless networks have to depend. As a result, denial of service on the satellite link, whether accidental or intentional, is a major concern. One of the very few security breaches documented to have affected an actual emergency response operation was a denial of service attack on the satellite link used by CISCO at the 2008 Evans Road Fire emergency in North Carolina. A fire-fighter's laptop that had been previously infected by trojan software started scanning as soon as it connected to the operation's HFN and launched a denial of service attack through the satellite link, which was quickly overwhelmed. Since then, CISCO has implemented egress filtering at each component network that is connected to the satellite and has introduced policies for authentication of users and regulated use of the

link [32]. This reduces the likelihood of accidental denial of service incidents, but it is unclear whether it would provide protection against intentional ones or availability attacks that are not based on flooding. This remains an open issue for research in EM satellite communications.

In addition, the security of confidentiality of communications using satellite phones has been contested by researchers. Driessen *et al.* [31] have recently reverse-engineered the encryption algorithms used in the GMR-1 and GMR-2 satellite phone standards and showed that their stream ciphers are considerably weaker than the current state of the art in symmetric cryptography. They have also developed a mechanism for recovering the encryption key of a GMR-2 phone call with approximately 50–65 bytes of key stream and moderate computational complexity. They have demonstrated this capability using low-cost commercial hardware and GNUradio-based software for receiving and filtering data. Thus, a second open issue is the development of stronger encryption algorithms that can be retrofitted on current satellite phones.

2.1.6. Wireless Communication Networks

In the immediate aftermath of large-scale disasters, such as the 2006 Yogyakarta earthquake in Japan and the 2004 tsunami that hit Aceh in Indonesia, the wired telecommunication network infrastructure is often completely destroyed and is often replaced by satellite communications (Section 2.1.5), wireless mesh (WMN), mobile ad hoc (MANET) and other wireless communication networks. Comprehensive surveys of cyber threats and defence mechanisms in general-use wireless networks can be found in [78] for WMNs and in [79] for MANETs. Here, we present the information security measures taken by wireless communication networks that have been recently designed specifically for use in emergencies.

The ability of wireless mesh networks (WMN) to self-heal, self-configure and provide wireless broadband connectivity at low cost makes them very attractive for public safety and crisis management communications. As a number of different emergency services need to collaborate during an operation, the requirement that is most frequently addressed in the literature is the secure access and sharing of information between multiple agencies, which may use different technologies and need to comply with different security policies. A common approach is to use cryptographic mechanisms for privacy, integrity, and authentication at the MAC layer, and IP Security (IPSec) or Transport Layer Security (TLS) at higher layers. For example, the GeoBIPS [33] self-forming broadband WMN, designed to be used by emergency reconnaissance teams and their commanding officers, serves as a relay network where privacy of voice and video communication is achieved through IPSec tunnelling. Each mobile access router is provided with a pre-shared authentication key used to sign all routing messages. Haji *et al.* [36] have proposed using both encryption and blocking of devices with physical addresses that are not on a predefined list of approved ones. Privacy can also be achieved through anonymity of the entities involved in the emergency operation [80], and crisis communication may be designed based on an unusual configuration of protocols and topology, so as to obfuscate or delay a potential intruder for the duration of the emergency [81]. Self-awareness and self-adaptation have been used extensively for network resilience, for example to reduce the impact of denial of service attacks [82] and worms [83]. These concepts have only recently been explored in the context of EM networks. In the EM MANET model presented in [37], the various security components are included, excluded, activated and deactivated dynamically based on real-time monitoring performed by an intrusion detection mechanism.

Bakat *et al.* [35] have proposed a centralised access control model for MANET-based emergency rescue operations, where each group of nodes has an allocated group leader node acting as the network's gateway. The architecture presented includes authentication, authorisation and cryptographic protocol layers, with an access control policy derived based on a hierarchical public key infrastructure for the group-role and user-role relationships. In addition, every member of the group is assigned a tag, which binds with a public key, a group and specified access privileges. Whenever a member of the group wishes to transmit data, the group leader needs to first verify the tag and a password.

However, as observed in [34], such protocols assume a pre-existing trust relationship between network nodes, which is not the case during major disasters where units from different emergency services need to communicate. In addition, the use of passwords or similar authentication mechanisms that require user input may be impractical in an emergency, where time is limited and human error is common. Gasoni and Paganelli [43] have suggested that in order to be fit for purpose, authentication in EM networks should be quick, scalable and extensible, requiring no human intervention or connection to a trusted third party. Their conclusion was that an "all-in-one" security device would be ideal. Such a Single Sign-On (SSO) technique has, in fact, been produced in [38], where the use of RFID accelerates authentication and automatic information retrieval. It additionally offers the flexibility of activating RFID tags only during the rescue missions and only for specified users. The RFID card can be deactivated immediately after a rescue mission, so as to minimise the impact of stolen cards. The specific framework has been designed for mobile communication between different agencies and includes a number of security measures. Communication between heterogeneous information providers is based on the Security Assertion Markup Language (SAML), and a Role Based Access Control (RBAC) model is used to control access rights. In addition, all entities communicate by using Secure Sockets Layer/Transport Layer Security with mutual authentication, as well as a logging service. The primary focus is on man-in-the-middle, replay and session hijacking attacks. The authors have developed a small scale prototype testbed to evaluate their framework in terms of performance, but have not evaluated its security in practice. Also, a security breach after the initial authentication, perhaps through social engineering, would leave the network vulnerable to an insider. Having got hold of a card, a malicious entity would be authenticated for a number of critical EM networks and services.

Yet, it is important to note that while authentication of users and devices may often not be ideal, it needs to be seen in conjunction with efficiency, safety and usability. As observed in [62], for emergency medical staff that may not already be authorised to access certain data, it might be better to have some form of second-factor authentication mechanism. This need for a more dynamic framework has been addressed in [39], where temporary access to sensitive data is authorised for first responders even if they have not been pre-vetted. The encryption mechanism is based on hardware security, and in particular on separation kernel technology and processor-internal encryption for data storage. Emergency information is stored and accessed in a special emergency partition, which is unavailable before the emergency and is purged after it finishes.

Open issues in Wireless Communication Networks used in EM: Considering that wireless communication mechanisms are often used in emergencies to address the availability issues of the damaged previous infrastructure, it is particularly interesting that there has been very little work in the literature related to the availability of these wireless EM systems. It is well known that availability

of wireless networks can easily be denied externally, for example by random channel jamming, or internally by the insider threat of a compromised node. In fact, WMN networks deployed in a disaster are considered to be more vulnerable to such insider threats than other types of wireless networks because they typically depend on low-cost devices with poor physical security [40]. Multi-hop wireless networks are vulnerable to masquerading or captured nodes that advertise themselves to the rest of the network as being on the shortest or most cost-efficient route to a destination, but instead of forwarding traffic, they drop some (grayhole attack) or all of it (blackhole attack). In the meantime, the affected nodes drain their batteries while resending the same traffic [42]. This effect can be achieved for TCP traffic simply by dropping a small percentage of consecutive packets, with what is known as a Jellyfish attack [40]. If the dropped packets are cumulative acknowledgements, then the transport layer interprets this as evidence of congestion and reduces the rate of transmission. Such attacks require very little energy on the part of the attacker and are difficult to detect. Yet, research on EM wireless security has focussed almost exclusively on authentication and access control for privacy, data integrity and data confidentiality rather than availability. Casoni and Paganelli [43] have suggested redundancy as the solution, but this is a costly approach, and prior experience in disaster zones has shown that the same physical event can take out redundant network nodes [84]. They have also proposed a simple policy and traffic shaping scheme that implements firewall and an intrusion detection system to counter availability attacks in an emergency MANET, but this approach requires powerful terminals rather than the mobile devices typically used by the emergency services.

Ensuring network availability in a wireless EM network, where no alternative or redundant technologies exist, remains a significant open issue. Relevant research on the availability specifically of EM opportunistic communications (Oppcomms) has been carried out by Gelenbe *et al.* [44]. Oppcomms are a type of delay/disruption-tolerant network where communication nodes store messages on behalf of others and forward them to other communication nodes when they meet. In practice, they provide a communication infrastructure in situations where connectivity is intermittent, which makes them naturally resilient to availability attacks. Nevertheless, cyber attacks can affect their performance considerably and severely impede the emergency operation. To evaluate this effect numerically, the specific team has adapted the distributed building evacuation simulator presented in [85] to investigate the impact of cyber attacks in the cyber-physical-human context of a technology-assisted evacuation [44]. Their simulation results have shown that even a single attacker can have significant impact on an evacuation that is heavily dependent on communications. To tackle this issue, they have proposed identity-based signatures and content-based message verification to block malicious traffic and nodes that could disrupt communications during a building evacuation. The mechanism is collaborative, with network nodes communicating with each other to establish the consistency of emergency information [41,86,87].

2.1.7. World Wide Web (WWW)

The WWW is used extensively to report damages, as well as for early warning and response. The Global Disaster Alert and Coordination System (GDACS) is used to provide real-time alerts about disasters around the world and tools to facilitate response coordination [15], while the Global Public Health Intelligence Network searches global media sources to identify disease outbreaks. At the same

time, the WWW is used to promote awareness and disseminate useful material, such as maps and training videos, especially for regions that are often hit by natural disasters. Specialised web content management systems, such as Synkron, SNAP [15] and the Food and Community Tracking System (FACTS), improve the efficiency of EM by facilitating collaboration between EM services, first responders and volunteers worldwide and on a day-to-day basis. However, all these systems depend on websites that can be attacked in a variety of manners. Simple denial of service attacks can knock them offline [88] and cross site scripting can be used to hijack legitimate users' accounts [64]. This would be particularly harmful if a disaster manager's account was hijacked, so as to broadcast rogue disaster alerts via SMS and email directly to the public, a capability that is available for example on the password-protected Virtual On-Site Operations Coordination Centre [15]. We have not identified any particular area of web security research that would be unique or more important in EM, and would not be covered in a generalist web security review paper. An excellent effort to formalise and categorise web security has been recently presented in [45] and a survey of current threats can be found in [46].

2.1.8. Social Media

Emergency services have been using web-based community warning systems for several years [89], and many have recently implemented social media strategies in their emergency response plans. This typically involves the local authorities broadcasting alerts to the followers of their twitter or Facebook accounts [90]. During the flooding in central Europe in 2010, the population of a city in Poland used a forum to exchange information about localised flooding, which was more efficient than the official communications using more traditional methods [91]. Twitter messages can potentially provide geo-location information, which would be invaluable, although still not widely in use in emergencies [92].

Most popular social networks rely exclusively on single login/password authentication. Their focus is primarily on privacy rather than security, despite the large number of high-profile incidents of hijacked accounts. Third party social media management applications are often used to improve on this security by providing differentiated permission levels and HTTPS for protecting from password sniffing on public wireless networks. However, there is no public study of their performance and effectiveness.

Open issues in security of Social Media used in EM: Individual accounts of social network users are often compromised, with plenty of web sites, Youtube videos and research papers showing how. An example is [47], which has discussed a series of methods for taking over Facebook and twitter accounts and for performing social network relay attacks on Facebook. In a relay attack, the attacker gets access to the social network content shared by the victim, creates a new profile with the same name as the victim, and selectively adds, deletes or modifies messages that are then shared with the public. So, it would not be unrealistic to consider an attacker gaining control of an emergency service's social network account to broadcast false information. This could endanger the public and impede emergency response, perhaps by initiating flash mobs of misled volunteers at an ill-chosen time and place.

In addition, there are currently projects piloted to allow the public to report emergencies using twitter and similar social networks instead of calling [93]. Thus, a second open issue has to do with the trustworthiness of information communicated by the public to the emergency services through social media. Hiltz and Gonzalez [48] have provided a first discussion on how to assess and improve the

trustworthiness of social media specifically for EM, but relevant technical research has not been provided to date.

At the same time, it is unclear how an EM social network-based reporting system would cope with large numbers of maliciously-generated spam messages. A first large-scale and systematic attempt to detect and defend against twitter spam has been recently presented in [49], where a Random Forest classifier is used to tell whether a message has been sent from a human, a bot, a human-assisted bot or a bot-assisted human. The latter refers to users employing applications that automatically post periodic updates in their absence. The classifier involves an entropy component that evaluates periodicity of message timing, a spam text Bayesian classification component looking for known spam text and a component that looks for suspicious account properties, as evidenced by the frequency and type of external URLs in tweets, the followers-to-friends ratio and the input device. The specific approach was shown to work particularly well when differentiating between humans and bots, but was less effective for human-assisted bots or bot-assisted humans. In addition, some of the input features used, such as signatures of known spam text and frequency of external URLs, would not be relevant in the case of an attack that aims to flood an emergency service's account with illegitimate or misleading messages rather than to advertise external links.

2.2. Sensing Technologies

Several EM tools for planning and decision making require reliable real-time information gathered through different sensing technologies. Here, we include satellite-based sensing, focussing on Global Positioning Systems (GPS), and terrestrial sensing with an emphasis on wireless sensor networks.

2.2.1. Satellite-Based Sensing

Polar-orbiting satellites provide good spatial resolution, but can update information on the same point only every few days because they fly in a low orbit. Geostationary satellites can provide updates every few minutes, but have lower spatial resolution as they fly at a much higher altitude. In EM, polar-orbiting satellites are used for operational planning and geostationary ones for the tracking of environmental changes and detection of impending natural disasters [15]. A satellite can host up to 5000 transponders for communication, each with the potential for permitting a cyber attack. Most satellites are custom built, which means that a cyber attack can only exploit a single system or very few systems. Kallberg *et al*. have argued that opportunities for covert activity and hijacking increases as more countries begin operating satellites, because vulnerabilities can be introduced through software updates and the onboard computer can be reconfigured [54].

The use of SDR in EM (Section 2.1.3) has provided potential attackers more options for compromising satellite communications and reducing the usability of GPS systems [27]. As EM systems make extensive use of GPS for geolocation, they are particularly vulnerable to spoofing attacks, where illegitimate signals deceive GPS receivers about their geographical coordinates. GPS spoofing can be more dangerous than jamming because the receiver remains unaware of the attack while false data are delivered to EM information management systems (Section 2.3) that depend heavily on GPS to coordinate operation planning and execution [51]. Tippenhauer *et al*. have provided an analysis of GPS

spoofing attacks with regard to their precision requirements [50] and Humphreys *et al*. have presented a portable GPS civilian spoofer in [94]. The latter have argued that it is less straightforward to defeat most user-equipment-based spoofing countermeasures if they use cryptographic authentication.

Unlike jamming, which can be quickly noticed by the victim, GPS spoofing is not easy to detect. Warner *et al*. have observed that GPS spoofing systems tend to use signals of much greater strength than legitimate GPS signals [52]. Thus, monitoring the signal strength should provide an indication of whether they are legitimate or spoofed. Signal quality monitoring techniques can effectively detect the spoofing correlation peak that is approaching the authentic signal, but are not applicable where spoofing does not affect the shape of the correlation peak, when spoofed and authentic signals are closely aligned. A solution to this problem was recently presented in [51], where detection is achieved based on amplitude analysis of different correlator branches. Spoofing is not only detected, but also mitigated, with a vector based tracking receiver structure that bridges the authentic signal outage. A different technique designed specifically to detect GPS spoofing attacks that affect the time synchronisation of wireless networks has been presented in [53]. Initial simulation results for both approaches have been promising, but none has been tested in a real world system yet.

2.2.2. Terrestrial Sensor Networks

Sensor networks are used for local environmental and safety monitoring, as well as in body area networks for health monitoring [95]. There are a number of ways for a cyber attack to affect an EM sensor network. It may aim to capture sensor nodes, inject bad data, disrupt connection or exhaust sensor batteries [56], so as to reduce the situational awareness of the first responders, delay the detection of an emergency and provide false or obsolete data to decision makers. The confidentiality of data from other nodes can be compromised with a sinkhole attack, where legitimate traffic is enticed through a compromised node [96] or with a Sybil attack, where fake identities are generated, so as to make multiple nodes appear using a number of different layers in the protocol stack [42]. The fake multiple identities can be used to vouch for one another to overcome cryptography techniques, as the node at the source of the attack may have access to multiple encryption keys [59,60]. The fake nodes can then send false link layer acknowledgements or inject false data into the network [97]. An excellent survey of the information security vulnerabilities of wireless sensor networks can be found in [98] and a survey of proposed defence mechanisms has been provided in [99]. Here, we will focus on research carried out specifically on the information security of sensor networks that have been used or proposed for EM.

Mitchell and Chen have used DHS Glanser to experiment on detection mechanisms that would be applicable to cyber-physical systems used in emergencies [56]. DHS Glanser is a collection of human-portable sensors and vehicle-mounted base stations used by the US emergency services. Their approach proposed in [57] uses a voting system to dynamically choose the optimal detection interval and number of sensor nodes participating in detection of cyber threats, based on a given set of false alarm probabilities and compromise rates. In principle, the approach that makes the best use of the dual nature of cyber-physical systems in EM is to use such data in combination with physical monitoring data. For example, by linking cyber detection with video surveillance and a central security room to monitor and report incidents, one may facilitate detection of suspicious cyber-physical behaviour [100]. Chen *et al* [58]. have proposed to use fuzzy logic to combine real-time network data and physical input

features, including the differences between the values reported by neighbouring sensors. It has been argued that in the cyber-physical systems of the near future, such as the ones currently proposed for emergency response, detection can only be effective if the behaviour of devices and users, as well as the inferred context, are integrated into the decision making process [101].

Open issues in Sensor Networks used in EM: The CodeBlue ad hoc sensor network infrastructure proposed in [61] for emergency medical care involves a decentralised security system that provides authentication and encryption. It implements an Elliptic Curve Cryptography-based system that takes up to 34 seconds to generate a key. The specific system may be prohibitively slow in an actual emergency, but improved light-weight cryptographic mechanisms that could be incorporated to body area networks have been proposed since and surveyed in [62]. Yet, it is interesting that wireless medical sensor networks used not only in EM, but generally in healthcare, have provisions only for authentication and privacy, as this is what is required for them to be accepted by the general public [102]. However, during an emergency these may be less important than availability. The intrusion detection mechanism for body area networks presented in [63] may be applicable, but it has been evaluated only in simulation. The protection of medical EM sensor networks against denial of service and other availability attacks remains an open issue for research.

2.3. Information Systems

From information gathering to planning and sharing of plans, EM operations depend heavily on EMIS that support interoperability between all functions and may involve multiple governmental organisations and the civilian population. Prior to an emergency, they are used to collect information for risk analysis, simulation of different scenarios and the development of contingency plans. During response and recovery they provide tools for the management and coordination of people and assets, as well as to improve transparency in aid. EMIS software may facilitate computerised modelling, prediction and risk analysis for the development of preparedness and contingency plans, and may be used to quantify the true cost of a disaster. During an actual emergency, they provide tools for managing the monitoring and warning networks, and for supporting decision-making, supervision, coordination of command and even context-aware emergency service streaming deliveries [103].

EMIS need to ensure the interoperability of all the functions they support [71], which implies the use of an inherent trust model within them [104]. Yet, EMIS typically consist of a combination of purpose-built and commercial off-the-shelf communication mechanisms and software, such as document readers, multimedia players and of course the operating system itself, each with their own and often well-known security flaws that make them vulnerable to malware and exploits. EMIS include or rely on geographic information systems (GIS) that use information generated through remote sensing for spatial analysis, interactive maps and hazard mapping, which can be vital to improve EM response times. GIS make extensive use of satellite tracking for accurate mapping (Section 2.2.1). They also use information through remote sensing for spatial analysis, interactive maps and hazard mapping. GIS often operate in conjunction with or based on cloud environments, such as third party web mapping services, and so effectively inherit cloud security threats. If the information that generates the map is modified, this will directly affect emergency response capability and planning [105]. Voice over IP (VoIP) is also

often employed in EMIS, but VoIP has not been designed for critical communications and is inherently insecure. An attacker can disrupt communication by flooding the VoIP servers or through the "Invite of Death" attack, leading to processing delays to VoIP traffic, unauthorised access and eventually denial of service [106]. A replay attack on the SIP protocols would cause the secured real time protocol to repeat the key stream used for media encryption, effectively breaking the transport layer security. Eavesdropping, spoofing and masquerading are very realistic threats in VoIP communication [66,67]. Where VoIP has been implemented as a soft phone, such as Skype, these soft phones have access to the system resources and hence the privileges of the user of the computer. Mechanisms for exploiting this have been presented in [68]. Policy-making, disaster planning, insurance risk analysis and EM scientific research rely heavily on databases with detailed information on previous disasters. Geospatial databases are also used to ensure transparency by tracking the aid received and by monitoring housing reconstruction programmes at the recovery phase. As with other software-based systems, off-the-shelf databases introduce known vulnerabilities in the EM process. When the target database system does not verify the input received from the user, SQL injection attacks can allow malicious users to both read and modify data [64,65].

The vulnerabilities described above are related to technologies used by EMIS rather than EM specific. In practice, security of EMIS has been gradually increased over the years. The US National EMIS (NEMIS) relied primarily on a single commercial off-the-shelf application security product that implemented RBAC assigned to the username [69], until a 2005 report revealed numerous failings in terms of user administration, server configuration, auditing, contingency training and testing. The report concluded that the Emergency Preparedness and Response Database did not have adequate security controls and there was an increased risk that unauthorised individuals could gain access to critical database resources and compromise the confidentiality, integrity and availability of sensitive NEMIS data. In addition, it might not be able to recover following a disaster. Seventy-one percent of the security enhancements suggested by this audit were soon implemented, but the remaining were deemed to have a negative impact on performance or were hindered by dependence on a commercial product [107]. At the most recent (June 2012) privacy impact assessment for key NEMIS modules related to the emergency recovery phase [108], the primary privacy risk identified was that information on individuals requesting assistance was not collected directly but through an intermediary body, thus increasing the chance of information being inaccurate, erroneously disclosed, retained for longer than necessary or used for purposes other than for what it was collected. NEMIS is still largely based on a RBAC architecture that restricts access to data or functionality in a manner pre-defined for each position and based on the principles of separation of duties and "need to know". This applies to both full-time personnel and first responders, as well as for contractors. Adam *et al*. [70] have presented an approach based on the RBAC model for information sharing within a virtual multi-agency response team. Their framework includes rules for admitting new agencies in the virtual team and a coordinator web service for each member to authenticate users, share information, create roles and enforce access control policies. Information sharing is secured through XML document encryption.

Open issues in EMIS security: Today, the most commonly discussed security requirement in EMIS is data confidentiality. As observed in [109], in life-threatening circumstances, many people would consider a loss of privacy a small price to pay. However, the interoperability of "systems of systems"

between different emergency services, the proliferation of personal data, and the society's increasing awareness of privacy intrusion, lead towards the need for "privacy by design" for EMIS. Busher *et al*. have argued that inscribing compliance into technologies is less useful due to the dynamic nature of emergency management, and that privacy should not be seen as a value that is traded in return for security, or as a right that has to be rigidly enforced [109]. Instead, they have emphasised on enhanced and comprehensive accountability and transparency, with the technological infrastructure of EMIS supporting not only access control and pre-defined rules, but also the mechanisms to trace the justification of inferences made during the disaster. This remains an open issue for research.

2.4. Vehicular Technologies

Like most modern vehicles, the manned vehicles used for transportation during an emergency include sophisticated computational and sensing technologies for their controls, and may soon include ad hoc vehicular networks supporting their communications. At the same time, there is increased interest in unmanned vehicles, for example for reaching locations that are inaccessible to humans. We have summarised related cyber threats in Table 4.

Table 4. Vehicular EM security threats and proposed countermeasures.

Technology	Security threat	Impact	Countermeasures
Manned Vehicles	Malware infection of traffic control systems [111]	Disabled air traffic control, signalling *etc*.	Web security literature [46]
	Malware infection of on board computers [113]	Hijacked control of locks, brakes and engine	Malware detection [113]
	GPS Spoofing [50,117]	Artificial traffic jam caused	Signal analysis [51–53]
	Web-based immobilisation hijacked [114]	Cars immobilised remotely and simultaneously	Web security literature [46]
Unmanned vehicles	GPS Spoofing [50,117]	Unmanned vehicle redirected [117,118]	Signal analysis [51–53]
	Gain-scheduling attack [117]	Control stability affected [117]	No known solutions
	Fuzzing attack [117]	Random inputs to vehicle's actuators [117]	No known solutions

2.4.1. Manned Vehicles

EM can be impaired by the means of transportation used by affected citizens, the emergency response vehicles used to carry people and equipment to and from the scene of the disaster, as well as by the local traffic.

In the public transport sector, cyber attacks usually cause disruption in dispatching and signalling. In the 1990s they were related primarily to the lack of user authentication mechanisms, with hackers connecting via a dial-up modem to an airport network pretending to be the legitimate system administrator and altering critical information. Today, computer viruses and targeted cyber attacks affecting mass transportation are relatively common, especially in railways and airports [110]. Due

to the increasing use of off-the-shelf computers running Microsoft Windows, a number of incidents in the transport sector were caused by common viruses and worms that spread via the Internet and infected computers indiscriminately, with one such virus disabling air traffic control systems in Alaska in 2006 [111]. Yet, in most cases, there was no malicious intent and, more significantly, there was no damage beyond frustration and financial costs due to downtime. In 2008 though, a teenager managed to take control of the tram system in Lodz, Poland, and operated its track switches, eventually causing four trains to derail and 14 people to be injured [112].

The automotive industry is also increasingly showing interest in cyber threats, partly because of isolated incidents of cyber intrusions against specific car types and partly thanks to the pioneering work of Koscher *et al*. [113]. In 2010, the latter demonstrated that it is possible to infect a car's networks via Bluetooth and other mechanisms and gain control of its locks, brakes and engine. A car interfered with in such a manner may be forced to veer towards one direction while driving at speed. While these vulnerabilities have been proven experimentally, we do not believe that they pose significant concern in the context of EM, as they do not scale easily enough to cause large-scale disruptions. On the other hand, an incident in Austin, Texas, the same year showed that large numbers of private cars can be simultaneously affected in an unexpected manner through a web-based vehicle-immobilisation system. The specific system had been set up by car dealers to disable a car's ignition system as a response to delinquent car payments, but it was exploited by a hacker who gained unauthorised access and issued rogue commands. Thus, it is particularly interesting that a website's security flaws had an indirect physical impact, causing 100 private cars to be simultaneously immobilised [114].

2.4.2. Unmanned Vehicles

Unmanned Aerial Systems (UAS) have already started being used for civilian purposes, including law enforcement and emergency response, as they can provide aerial imagery of high resolution that enhances situational awareness and coordination. However, the security of unmanned aerial vehicles (UAVs) has been repeatedly breached in high-profile incidents in the past. In 2009, militants in Iraq used cheap off-the-shelf software to intercept live video feeds from US Predator drones and in 2011 a virus infected a number of US Predator and Reaper UAV drones, logging the keystrokes of the pilots who remotely controlled them [115]. The same year, Iranian TV showed a US RQ-170 Sentinel drone claiming that it had been electronically hijacked and landed by the Iranian army's electronic warfare unit [116]. According to [105], this was achieved by spoofing the GPS signals to the drone and then tricking it into landing in Iran rather than Afghanistan. The drone reported that it was landing at its home base. It is important to note that as UAVs are sizeable objects, if hijacked and deliberately crashed into a crowd or other target, they could cause considerable physical damage themselves.

The elevated significance of UAV hijacking in the defence sector has sparked research in UAV cyber security. Most notably, a research team in Purdue University has created a simulation testbed that models UAV control systems and flight operations. Their current primary focus is on vulnerabilities of the autopilot systems. Up to now, they have confirmed that GPS spoofing can lead a UAV astray and in manner that may not be detected by the legitimate operator. In addition, they have analysed a gain-scheduling attack affecting the vehicle's controls and stability through sensor spoofing, and a fuzzing attack where the attacker injects random inputs to the vehicle's actuators [117]. In parallel, a

less technical high-level analysis of the potential impact of cyber attacks on UAVs has been presented in [118]. It is important to note that a recent congressional report on unmanned aircraft systems has stated that vulnerabilities in the command and control of UAS operations are a primary obstacle to their integration in the national airspace system [119].

Land vehicles that operate in an autonomous or semi-autonomous remotely-controlled manner are also increasingly proposed and trialled for EM. Such vehicles can reach areas often inaccessible to first responders and even set up an ad hoc communication infrastructure [120]. However, unmanned vehicles are typically not designed with information security in mind and are vulnerable to multiple types of attacks affecting the collection or communication of critical information. An excellent survey of these cyber threats has been presented in [121].

Open issues in Vehicular Technologies used in EM: While we do not consider the vulnerabilities of embedded vehicular systems or web-based immobilisation systems to be an imminent cause for concern in EM, threats from other supporting technologies, such as satellite navigation systems, could have a more serious and direct impact. Potential manipulation of satellite navigation signals (Section 2.2.1) could affect EM by creating local congestion so as to maximise the number of civilians affected by a terrorist attack or to delay ambulances and fire engines, and such attacks have already been shown to affect UAVs. While research in anti-spoofing mechanisms for satellite navigation has been carried out (Section 2.2.1), these are unlikely to be implemented in real world systems very soon. Thus, the impact that cyber-initiated traffic congestion or UAS hijacking would have in an emergency needs to be analysed.

3. A Grand Challenge in EM Security

The principles of information security apply to EM systems in the same way they apply to any other ICT infrastructure. The confidentiality of streamed media or patient data, the integrity of command and control channels, the availability of network connectivity and the authenticity of user input need to be upheld to a reasonable degree. We argue that the grand challenge is to identify what reasonable security actually means for a given EM scenario. In order to take an informed decision, one needs to have evaluated the impact and likelihood of a potential attack against the performance or accessibility overhead of a proposed defence. Thus, we believe that a key challenge for EM security is to develop the necessary tools to be able to evaluate this trade-off in the context of particular EM operations.

3.1. Prediction and Evaluation of a Cyber Attack's Impact on EM

Current EMIS systems provide tools for predicting the evolution of an emergency based on the physical characteristics of the environment and the nature of the emergency. They do not take into account the impact of cyber failures, intentional or not. We argue that EMIS need to evaluate the impact of cyber threats on the mitigation, preparedness, response and recovery phases of EM, from the likelihood of a disaster to occur, up to the financial loss and the number of casualties caused by it. A similar recently developed research area in the defence sector is the mission impact analysis of cyber threats. For example, a first example of a cyber impact dependency graph model has been provided in [122] to evaluate the effect that a cyber attack has on the operational capacity of an ongoing military

mission, and Tadda *et al*. [123] have discussed mission impact and cyber threat assessment in the military context. However, these pieces of research are still at an early stage and do not necessarily translate well in the EM setting where the civilian population is directly affected and the technologies involved are different.

Nearer this goal is the research carried out by Gelenbe *et al*. [44], who have been using an EM simulation environment to evaluate the impact of cyber attacks on an actual building evacuation mission. In their simulations, they have measured the ratio of evacuated civilians and the average evacuee health against the number of malicious nodes participating in a cyber attack that aims to disrupt the coordination of the mission. We believe that the analysis of cyber threats in this manner is in the right direction, because impact is measured in real-world metrics, such as number of casualties, rather than only cyber metrics. The grand challenge is to scale up this type of analysis to be able to take into account the whole operational picture and the cyber-physical-human interdependencies between different technologies, different emergency services and agents, as well as the evolving physical environment. For this, new large-scale EM augmented simulation environments and mathematical models may be needed.

4. Conclusions

The effectiveness of modern emergency management relies on the uninterrupted operation of a range of information and communication systems. As several researchers have observed [87,124,125], a cyber attack can be used to assist terrorist activities by softening a target before a physical attack or by generating fear and confusion. Yet, the majority of research for the security of EM systems has focussed on preventive approaches that assume that an authentication framework based on encryption of communications and access control will always be successful, and are not complemented by reactive response mechanisms (Table 5).

It is reasonable to assume that a dedicated cyber criminal who would aim to assist a concurrent physical attack would possibly employ social engineering to bypass authentication or denial of service attacks that would target the availability rather than the confidentiality or integrity of the EM infrastructure. Although availability of communications has been consistently presented as a key issue in a combined cyber-physical terrorist attack [18], there is still a remarkable lack of relevant EM-specific defence solutions that have progressed beyond the level of conceptual analysis.

In this paper, we have provided a review of the related cyber threats and their impact on the EM technologies affected, emphasising on the open issues for research. We have argued that a grand challenge for EM security is the development of tools that would help us analyse and predict the actual impact of such cyber threats on the four phases of EM, from the likelihood of a disaster to occur, up to the financial loss and the number of casualties caused by it.

Table 5. Overview of research on analysis and countermeasures for EM cyber threats.

	Platform				Category				Impact			Countermeasures				
	Conceptual	**Mathematical**	**Simulation**	**Prototype/Experim.**	**Communications**	**Sensing**	**EMIS**	**Vehicular**	**Confidentiality**	**Integrity**	**Availability**	**Authentication**	**Resilience**	**Detection**	**Response**	**Procedural**
Adam *et al.* [70]		x		x	x				x			x				
Al Ameen *et al.* [102]	x				x	x			x	x		x				
Bakar *et al.* [35]	x	x			x				x	x		x				x
Belala *et al.* [126]				x	x	x			x			x				
Bharania [32]				x	x				x	x	x	x		x		x
Bouckaert [33]				x	x				x	x		x				
Casoni and Paganelli [43]	x				x				x	x	x	x	x	x		
Chan *et al.* [25]		x			x	x				x	x	x	x	x		x
Chow *et al.* [101]	x				x			x						x		
Chu *et al.* [48]			x	x	x					x				x		
Clark *et al.* [29]		x		x	x				x	x						
De Cerchio and Riley [111]	x							x	x	x	x					
DHS/FEMA [108]	x						x		x							x
Gelenbe *et al.* [41,44,86,87]			x	x	x	x			x	x	x	x	x	x	x	x
Haji *et al.* [36]	x				x	x			x			x				
Hiltz and Gonzalez [48]	x				x					x						
Jafarnia-Jahromi *et al.* [51]			x		x					x				x	x	
Jakobson [122]	x				x	x	x	x	x	x	x					
Javaid *et al.* [118]	x							x	x	x	x					
Kim *et al.* [117]			x					x	x	x	x					
Levin *et al.* [39]	x						x		x	x		x				x
Li *et al.* [62]	x				x	x			x			x				
Liu *et al.* [26]		x	x		x	x					x		x		x	
Malan *et al.* [61]				x	x	x			x	x		x				
Michalas *et al.* [80]		x		x	x				x			x				
Mitchell *et al.* [56,57]		x			x	x		x	x	x				x		
Rafique *et al.* [106]				x			x				x					
Rao and Rao *et al.* [55]			x		x	x					x		x			
Storey [112]	x							x		x						
Tran *et al.* [38]			x		x				x			x				x
Walker *et al.* [18,71]	x				x	x	x	x	x	x	x					x
Warner *et al.* [52]	x				x						x			x	x	
Zeng *et al.* [53]			x		x					x				x		

References

1. Bahrepour, M.; Meratnia, N.; Poel, M.; Taghikhaki, Z.; Havinga, P.J.M. Distributed Event Detection in Wireless Sensor Networks for Disaster Management. In Proceedings of the 2nd International Conference on Intelligent Networking and Collaborative Systems, Thessaloniki, Greece, 24–26 November 2010; pp. 507–512.
2. Gelenbe, E.; Wu, F.J. Sensors in Cyber-Physical Emergency Systems. In Proceedings of the IET Conference on Wireless Sensor Systems, London, UK, 18–19 June 2012.
3. Filippoupolitis, A.; Hey, L.; Loukas, G.; Gelenbe, E.; Timotheou, S. Emergency Response Simulation Using Wireless Sensor Networks. In Proceedings of the The 1st International Conference on Ambient Media and Systems, Quebec, Canada, 11–14 February 2008.
4. Du, C.; Zhu, S. Research on urban public safety emergency management early warning system based on technologies for the Internet of things. *Procedia Eng.* **2012**, *45*, 748–754.
5. Delle Fave, F.M.; Rogers, A.; Jennings, N.R. ARGUS: A Coordination System to Provide First Responders with Live Aerial Imagery of the Scene of a Disaster (Demonstration). In Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems, Valencia, Spain, 4–8 June 2012; Volume 3, pp. 1467–1468.
6. Timotheou, S.; Loukas, G. Autonomous Networked Robots for the Establishment of Wireless Communication in Uncertain Emergency Response Scenarios. In Proceedings of ACM Symposium on Applied Computing, Hawaii, USA, 8–12 March 2009; pp. 1171–1175.
7. White, C.; Plotnick, L.; Hiltz, S.R.; Turoff, M. An online social network for emergency management. *Int. J. Emerg. Manag.* **2009**, *6*, 369–382.
8. Yates, D.; Paquette, S. Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *Int. J. Inf. Manag.* **2011**, *31*, 6–13.
9. Dudenhoeffer, D.; Permann, M.; Manic, M. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In Proceedings of the 2006 IEEE Winter Simulation Conference,Monterey, CA, USA, 3–6 December 2006; pp. 478–485.
10. Dudenhoeffer, D.D.; Permann, M.R.; Woolsey, S.; Timpany, R.; Miller, C.; McDermott, A.; Manic, M. Interdependency Modeling and Emergency Response. In Proceedings of the 2007 Summer Computer Simulation Conference, San Diego, CA, USA, 15–18 July 2007; SCS: San Diego, CA, USA; pp. 1230–1237.
11. Loukas, G.; Gan, D.; Vuong, T. A Taxonomy of Cyber Attack and Defence Mechanisms for Emergency Management Networks. In Proceedings of the Third International Workshop on Pervasive Networks for Emergency Management (IEEE PerNem 2013), San Diego, CA, USA, 18–22 March 2013.
12. Crondstedt, M. Prevention, preparedness, response, recovery—An outdated concept? *Aust. J. Emerg. Manag.* **2002**, *17*, 10–13.

13. Gianni, D.; Loukas, G.; Gelenbe, E. A Simulation Framework for the Investigation of Adaptive Behaviours in Largely Populated Building Evacuation Scenarios. In Proceedings of the Seventh International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS 08), Estoril, Portugal, 12–16 May 2008.
14. Galea, E.R.; Sharp, G.; Lawrence, P.J.; Holden, R. Approximating the evacuation of the World Trade Center north tower using computer simulation. *J. Fire Prot. Eng.* **2008**, *18*, 85–115.
15. Apikul, C. ICT for disaster risk reduction in Asia and the Pacific. In *ICT for Disaster Risk Reduction, ICTD Case Study 2*; Asian and Pacific Training Centre for Information and Communication Technology for Development: Incheon, Korea, 2010; pp. 10–49.
16. Mankovich, N.; Fitzgerald, B. Managing Security Risks with 80001. In *Advancing Safety in Medical Technology Conference and Expo*; Association for the Advancement of Medical Instrumentation: Arlington, VA, USA, 2011.
17. Harries, D.; Yellowlees, P.M. Cyberterrorism: Is the U.S. healthcare system safe? *Telemed. e-Health* **2012**, *19*, 1–6.
18. Walker, J. Cyber Security Concerns for Emergency Management. In *Emergency Management*; Eksioglu, B., Ed.; InTech: Rijeka, Croatia, 2012; pp. 39–59.
19. Falcarin, P.; Collberg, C.; Atallah, M.; Jakubowski, M. Guest editors' introduction: Software protection. *IEEE Softw.* **2011**, *28*, 24–27.
20. Madhava, S.S.P.; Jaishankar, K. Cyber Terrorism: Problems, Perspectives and Prescription. In *Crimes of the Internet*; Schmallager, F., Pittaro, M., Eds.; The ACM Digital Library: New York, NY, USA, 2008; pp. 593–611.
21. Traynor, P. Characterizing the security implications of third-party emergency alert systems over cellular text messaging services. *IEEE Trans. Mob. Comput.* **2012**, *11*, 983–994.
22. Fournier, J.-C.; Rose, S. Message Transmission System and Method, and Utilization of the Transmission System to Investigate Services Offered. US Patent 7,130,648, 31 October 2006.
23. Kristiansson, U.; Osth, K.-J.; Blomqvist, E.; Claassen, G. Method and Apparatus for Transmitting Secure Cell Broadcast Messages in a Cellular Communication Network. WIPO Patent Application WO/2012/108803, 18 June 2012.
24. Tague, P.; Li, M.; Poovendran, R. Mitigation of control channel jamming under node capture attacks. *IEEE Trans. Mob. Comput.* **2009**, *8*, 1221–1234.
25. Chan, A.; Liu, X.; Noubir, G.; Thapa, B. Broadcast Control Channel Jamming: Resilience and Identification of Traitors. In Proceedings of the IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2007; pp. 2496–2500.
26. Liu, S.; Lazos, L.; Krunz, M. Thwarting control-channel jamming attacks from inside jammers. *IEEE Trans. Mob. Comput.* **2012**, *11*, 1545–1558.
27. Jones, G. Mobile menace: Why SDR poses such a threat. *Netw. Secur.* **2012**, *6*, 5–7.
28. Park, Y.S.; Kim, C.S.; Ryou, J.C. The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol. In Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT), Gangwon-Do, Korea, 7–10 February 2010; pp. 1469–1473.

29. Clark, S.; Metzger, P.; Wasserman, Z.; Xu, K.; Blaze, M.A. *Security Weaknesses in the APCO Project 25 Two-Way Radio System*; Technical Report MS-CIS-10-34; University of Pennsylvania: Philadelphia, PA, USA, 2010.
30. Glass, S.; Muthukkumarasamy, V.; Portmann, M.; Robert, M. Insecurity in Public-Safety Communications: APCO Project 25. In Proceedings of the 7th International ICST Conference on Security and Privacy in Communication Networks, SecureComm 2011, London, UK, 7–9 September 2011.
31. Driessen, B.; Hund, R; Willems, C.; Paar, C.; Holz, T. Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Diego, CA, USA, 20–23 May 2013; pp. 128–143.
32. Bharania, R. Securing Hastily Formed Networks for Disaster Relief and Emergency Response. Presented at CISCO Live, San Diego, CA, USA, 10–14 June 2012.
33. Bouckaert, S.; Bergs, J.; Naudts, D. A Mobile Crisis Management System for Emergency Services: From Concept to Field Test. In Proceedings of the 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, Waterloo, Canada, 7–9 August 2006.
34. Portmann, M.; Pirzada, A.A. Wireless mesh networks for public safety and crisis management applications. *IEEE Internet Comput.* **2008**, *12*, 18–25.
35. Bakar, A.; Roslan, I.; Ahmad, A.R.; Abd Manan, J.-L. Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission. In Proceedings of the International Conference on Information and Knowledge Management (ICIKM), Kuala Lumpur, Malaysia, 24–26 July 2012.
36. Haji, R.; Hasbi, A.; Ghallali, M.; El Ouahidi, B. Towards an Adaptive QoS-Oriented and Secure Framework for Wireless Sensor Networks in Emergency Situations. In Proceedings of the International Conference on Multimedia Computing and Systems, Tangier, Morocco, 10–12 May 2012; pp. 1007–1011.
37. De Oliveira, T.R.; de Oliveira, S.; Macedo, D.F.; Nogueira, J.M. An Adaptive Security Management Model for Emergency Networks. In 7th Latin American Network Operations and Management Symposium (LANOMS), Quito, Ecuador, 10–11 October 2011.
38. Tran, T.; Yousaf, F.Z.; Wietfeld, C. RFID-Based Secure Mobile Communication Framework for Emergency Response Management. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Sydney, Australia, 18–21 April 2010.
39. Levin, T.E.; Irvine, C.E.; Benzel, T.V; Nguyen, T.D.; Clark, P.C.; Bhaskara, G. Idea: Trusted Emergency Management. In *Engineering Secure Software and Systems (ESSoS)*; Springer-Verlag: Berlin, Germany, 2009; pp. 32–36.
40. Lazos, L.; Krunz, M. Selective jamming/dropping insider attacks in wireless mesh networks. *IEEE Netw.* **2011**, *25*, 30–34.
41. Gorbil, G.; Gelenbe, E. Resilience and Security of Opportunistic Communications for Emergency Evacuation. In Proceedings of the 7th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks (PM2HW2N'12), Paphos, Cyprus, 21–22 October 2012; pp. 115–124.

42. Liao, X.; Hao, D.; Sakurai, K. Classification on Attacks in Wireless Ad Hoc Networks: A Game Theoretic View. In Proceedings of 7th International Conference on Networked Computing and Advanced Information Management (NCM), Gyeongju, Korea, 21–23 June 2011.
43. Casoni, M. and Paganelli, A. Security Issues in Emergency Networks. In Proceedings of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC), Istanbul, Turkey, 4–8 July 2011; pp. 2145–2150,
44. Gelenbe, E.; Gorbil, G.; Wu, F.-J. Emergency Cyber-Physical-Human Systems. In Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 June–2 August 2012.
45. Akhawe, D.; Barth, A.; Lam, P.E.; Mitchell, J.; Song, D. Towards a Formal Foundation of Web Security. In Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF), Edinburgh, Scotland, UK, 17–19 July 2010; pp. 290–304.
46. Jensen, M.; Gruschka, N.; Herkenhöner, R. A survey of attacks on web services. *Comput. Sci.-Res. Dev.* **2009**, *24*, 185–197.
47. Mahmood, S. New Privacy Threats for Facebook and Twitter Users. In Proceedings of the Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Victoria, Canada, 12–14 November 2012; pp. 164–169.
48. Hiltz, S.R.; Gonzalez, J.J. Assessing and Improving the Trustworthiness of Social Media for Emergency Management: A Literature Review. In Proceedings of the Norwegian Information Security Conference (NISK), Bodo, Norway, 19–21 November 2012.
49. Chu, Z.; Gianvecchio, S.; Wang, H.; Jajodia, S. Detecting automation of twitter accounts: Are you a human, bot or cyborg? *IEEE Trans. Dependable Secur. Comput.* **2012**, *9*, 811–824.
50. Tippenhauer, N.O.; Popper, C.; Rasmussen, K.B.; Capkun, S. On the Requirements for Successful GPS Spoofing Attacks. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; ISBN: 978-1-4503-0948-6, pp. 75–86.
51. Jafarnia-Jahromi, A.; Lin, T.; Broumandan, A.; Nielsen, J.; Lachapelle, G. Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver, ION ITM 2012, Newport Beach, CA, 30 January–1 February 2012.
52. Warner, J.S.; Johnston, R.G. GPS Spoofing Countermeasures. *Homel. Secur. J.* **2003**, *LAUR-03-6163*, 22–30.
53. Zeng, Q.; Li, H.; Qian, L. GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design. In Proceedings of the Military Communications Conference (MILCOM), Orlando, FL, USA, 29 October–1 November 2012.
54. Kallberg, J. Designer satellite collisions from covert cyber war. *Strateg. Stud. Q.* **2012**, 124–136.
55. Rao, G.K.; Rao, R.S.H. Status Study on Sustainability of Satellite Communication Systems Under Hostile Jamming Environment. In Proceedings of 2011 Annual IEEE India Conference (INDICON), Hyderabad, India, 16–18 December 2011; pp. 1–7.
56. Mitchell, R.; Chen, I.R. A Hierarchical Performance Model for Intrusion Detection in Cyber-Physical Systems. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Cancun, Mexico, 28–31 March 2011; pp. 2095–2100.

57. Mitchell, R.; Chen, I.R. Survivability Analysis of Mobile Cyber Physical Systems with Voting-Based Intrusion Detection. In Proceedings of the 7th International Wireless Communications and Mobile Computing Conference (IWCMC), Istanbul, Turkey, 4–8 July 2011; ISBN 978-1-4244-9539-9.
58. Chen, Y.J.; Shih, J.S.; Cheng, S.T. A Cyber-Physical Integrated Security Framework with Fuzzy Logic Assessment for Cultural Heritages. In Proceeding of the IEEE International Conference on Systems, Man and Cybernetics, Anchorage, AK, USA, 9–12 October 2011; ISBN 978-1-4577-0652-3, pp. 1843–1847.
59. Pramod, A.V.; Azeem, M.A.; Prakash, M.O. Detecting the sybil attack in wireless sensor network. *Int. J. Comput. Technol.* **2012**, *3*, 158–161.
60. Conti, M.; Di Pietro, R.; Mancini, L.V.; Mei, A. Distributed detection of clone attacks in wireless sensor networks. *IEEE Trans. Dependable Secur. Comput.* **2011**, *8*, 685–698.
61. Malan, D.; Fulford-Jones, T.; Welsh, M.; Moulton, S. Codeblue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. In Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks, London, UK, 3–5 April 2004.
62. Li, M.; Lou, W.; Ren, K. Data security and privacy in wireless body area networks. *IEEE Wirel. Commun.* **2010**, *17*, 51–58.
63. Sundararajan, T.V.P.; Shanmugam, A. A novel intrusion detection system for wireless body area network in health care monitoring. *J. Comput. Sci.* **2010**, *6*, 1355–1361.
64. Kindy, D.A.; Pathan, A.K. A Survey on SQL Injection: Vulnerabilities, Attacks, and Prevention Techniques. In Proceedings of the IEEE International Symposium on Consumer Electronics, Singapore, 14–17 June 2011; pp. 468–471.
65. Cecchini, S.; Gan, D. The AMP attacker: A suite of tools for exploiting SQL injection vulnerabilities in web applications. *Int. J. Electron. Secur. Digit. Forensics* **2013**, in press.
66. Ehlerta, S.; Geneiatakis, D.; Magedanza, T. Survey of network security systems to counter SIP-based denial-of-service attacks. *Comput. Secur.* **2010**, *29*, 225–243.
67. Rezac, F.; Voznak, M. Security risks in IP telephony. *Adv. Electr. Electron. Eng.* **2011**, *8*, 15–23.
68. Dantu, R.; Fahmy, S.; Schulzrinne, H.; Cangussu, J. Issues and challenges in securing VoIP. *Comput. Secur.* **2009**, *28*, 743–753.
69. Federal Emergency Management Agency (FEMA). *National Emergency Management Information System Concept of Operations*; Diane Co.: Washington, DC, USA, 1998.
70. Adam, N.; Kozanoglu, A; Paliwal, A.; Shafiq, B. Secure information sharing in a virtual multi-agency team environment. *Electron. Notes Theor. Comput. Sci.* **2007**, *179*, 97–109.
71. Walker, J.; Williams, B.J.; Skelton, G.W. Cyber Security for Emergency Management. In IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 8–10 November 2010; pp. 476–480.
72. Traynor, P.; Enck, W.; McDaniel, P.; La Porta, T. Exploiting open functionality in SMS-capable cellular networks. *J. Comput. Secur.* **2008**, *16*, 393–404.
73. Traynor, P.; Enck, W.; McDaniel, P.; La Porta, T. Mitigating attacks on open functionality in SMS-capable cellular networks. *IEEE/ACM Trans. Netw.* **2009**, *17*, 182–193.

74. Karaliopoulos, M.; Henrio, P.; Mazzella, M.; de Win, W.; Dieudonne, M.; Andrikopoulos, I.; Mertzanis, I.; Corazza, G.E.; Vanelli-Coralli, A.; Dimitriou, N.; Polydoros, A. Satellite radio interface and radio resource management strategy for the delivery of multicast/broadcast services via an integrated satellite-terrestrial system. *IEEE Commun. Mag.* **2004**, *42*, 108–117.
75. Vojcic, B.; Matheson, D.; Clark, H. Network of Mobile Networks: Hybrid Terrestrial-Satellite Radio. In Proceedings of the International Workshop on Satellite and Space Communications, Siena, Italy, 9–11 September 2009; pp. 451–455.
76. Lee, Y.-M.; Ku, B.-J.; Ahn, D.-S. A Satellite Core Network System for Emergency Management and Disaster Recovery. In Proceedings of the 2010 International Conference on Information and Communication Technology Convergence, Jeju Island, Korea, 17–19 November 2010; pp. 549–552.
77. Nelson, C.; Steckler, B.D.; Stamberger, J.A. The Evolution of Hastily Formed Networks for Disaster Response. In Proceedings of Global Humanitarian Technology Conference, IEEE, Seattle, WA, USA, 30 October–1 November 2011.
78. Yi, P.; Wu, Y.; Zou, F.; Liu, N. A survey on security in wireless mesh networks. *IETE Tech. Rev.* **2010**, *27*, 6–14.
79. Wu, B.; Chen, J.; Wu, J.; Cardei, M. A survey of attacks and countermeasures in mobile ad hoc networks. *Wirel. Netw. Secur.* **2007**, 103–135.
80. Michalas, A.; Bakopoulos, M.; Komninos, N.; Prasad, N.R. Secure and Trusted Communication in Emergency Situations. In Proceedings of the 35th IEEE Sarnoff Symposium (SARNOFF), Newark, NJ, USA, 21–22 May 2012; pp. 228–232.
81. Collberg, C.; Thomborson, C. Watermarking, tamper-proofing, and obfuscation-tools for software protection. *IEEE Trans. Softw. Eng.* **2002**, *28*, 735–746.
82. Gelenbe, E.; Loukas, G. A self-aware approach to denial of service defence. *Comput. Netw.* **2007**, *51*, 1299–1314.
83. Sakellari, G.; Gelenbe, E. Demonstrating Cognitive Packet Network Resilience to Worm Attacks. In Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; ISBN 978-1-4503-0245-6, pp. 636–638.
84. Sterbenz, J.P.G.; Cetinkaya, E.K.; Hameed, M.A.; Jabbar, A.; Qian, S.; Rohrer, J.P. Evaluation of network resilience, survivability, and disruption tolerance: Analysis, topology generation, simulation, and experimentation. *Telecommun. Syst.* **2011**, 1–34; doi:10.1007/s11235-011-9573-6.
85. Filippoupolitis, A.; Loukas, G.; Timotheou, S.; Dimakis, N.; Gelenbe, E. Emergency Response Systems for Disaster Management in Buildings. In Proceedings of NATO Symposium on C3I for Crisis, Emergency and Consequence Management, Bucharest, Romania, 11–12 May 2009.
86. Gorbil, G.; Gelenbe, E. Disruption Tolerant Communications for Large Scale Emergency Evacuation. In Proceedings of the 11th IEEE International Conference on Pervasive Computing and Communication, San Diego, CA, USA, 18–22 March 2013.
87. Gorbil, G.; Gelenbe, E. Resilient Emergency Evacuation Using Opportunistic Communications. In *Computer and Information Sciences III*; Gelenbe, E., Lent, R., Ed.; Springer: Berlin, Germany, 2013; pp. 249–257.

88. Loukas, G.; Oke, G. Protection against denial of service attacks: A survey. *Comput. J. Br. Comput. Soc.* **2010**, *53*, 1020–1037.
89. Bunker, D.; Smith, S. Disaster Management and Community Warning Systems: Inter-Organisational Collaboration and ICT Innovation. In Proceedings of the Pacific Asia Conference on Information Systems, Hyderabad, India, 10–12 July 2009.
90. Magsino, S.L. *Applications of Social Network Analysis for Building Community Disaster Resilience*; The National Academies Press: Washington, DC, USA, 2009.
91. Wojciechowicz, W.; Zych, J.; Hołubowicz, W. Information and communication technology and crisis management. *Tech. Sci.* **2012**, *15*, 101–110.
92. Kreiner, K.; Neubaur, G. Social Media for Crisis Management: Problems and Challenges from an IT-Perspective. In Proceedings of Interdisciplinary Information and Management Talks IDIMT 2012, Jindřichův Hradec, Czech Republic, 12–14 September 2012.
93. Roitman, H.; Mamou, J.; Mehta, S.; Satt, A.; Subramaniam, L.V. Harnessing the Crowds for Smart City Sensing. In Proceedings of the 1st International Workshop on Multimodal Crowd Sensing, Maui, Hawaii, USA, 29 October–2 November 2012; pp. 17–18.
94. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M., Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of ION GNSS Conference, Institute of Navigation, Savanna, GA, USA, 16–19 September 2008.
95. Lorincz, K.; Malan, D.J.; Fulford-Jones, T.E.F.; Nawoj, A.; Clavel, A.; Shnayder, V.; Mainland, G.; Welsh, M. Sensor networks for emergency response: Challenges and opportunities. *IEEE Pervasive Comput.* **2004**, *3*, 16–23.
96. Skelton, G.W. Cyber-Physical Security for Wireless Sensor Networks. In Proceedings of the Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, USA, 22–24 July 2009.
97. Lin, J.; Yu, W.; Yang, X.; Xu, G.; Zhao, W. On False Data Injection Attacks against Distributed Energy Routing in Smart Grid. In Proceedings of the ACM/IEEE Third International Conference on Cyber-Physical Systems, Beijing, China, 17–19 April 2012.
98. Kavitha, T.; Sridharan, D. Security vulnerabilities in wireless sensor networks: A survey. *J. Inf. Assur. Secur.* **2010**, *5*, 31–44.
99. Zhou, Y.; Fang, Y.; Zhang, Y. Securing wireless sensor networks: A survey. *Commun. Surv. Tutor. IEEE* **2008**, *10*, 6–28.
100. Rajamaki, J.; Rathod, P.; Ahlgren, A.; Aho, J.; Takari, M.; Ahlgren, S. Resilience of Cyber-Physical System: A Case Study of Safe School Environment. In Proceedings of the Intelligence and Security Informatics Conference (EISIC), Odense, Denmark, 22–24 August 2012.
101. Chow, R.; Uzun, E.; Cardenas, A.A.; Song, Z.; Lee, S. Enhancing Cyber-Physical Security through Data patterns. In Proceedings of the Workshop on Foundations of Dependable and Secure Cyber-Physical Systems, Chicago, IL, USA, 11 April 2011.
102. Al Ameen, M.; Liu, J.; Kwak, K. Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.* **2012**, *36*, 93–101 .

103. Mejia Bernal, J.F.; Ardito, L.; Falcarin, P.; Rodriguez Rocha, O.; Morisio, M.; Giovannelli, F.; Pistore, F. Emergency situations supported by context-aware and application streaming. *Int. J. Ad Hoc Ubiquitous Comput.* **2013**, *13*, in press.
104. Gao, Y.; Li, C.; Zhao, Y. The Review of Emergency Management Research. In Proceedings of the 2nd IEEE International Conference on Emergency Management and Management Sciences (ICEMMS), Beijing, China, 8–10 August 2011; pp. 732–736.
105. Racek, J.; Ministr, J. ICT Support for Emergency Management. In Proceedings of Interdisciplinary Information and Management Talks IDIMT 2012, Jindřichův Hradec, Czech Republic, 12–14 September 2012,
106. Rafique, M.Z. Akabar, M.A.; Farooq, M. Evaluating DoS Attacks Against SIP-Based VoIP Systems. In Proceedings of IEEE GLOBECOM, Honolulu, HI, USA, 30 November–4 December 2009.
107. Department of Homeland Security (DHS). *Security Weaknesses Increase Risks to Critical Emergency Preparedness and Response Database*; OIG-05-43; Office of Information Technology: Washington, DC, USA, 2005.
108. Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA). *Privacy Impact Assessment for the National Emergency Management Information System—Individual Assistance (NEMIS-IA) Web-Based and Client-Based Modules*; DHS/FEMA/PIA-027; DHS/FEMA: Washington, DC, USA, 2012.
109. Buscher, M.; Wood, L.; Perng, S.Y. Privacy, Security, Liberty: Informing the Design of EMIS. In Proceedings of the 10th International ISCRAM Conference, Baden-Baden, Germany, 12–15 May 2013.
110. Turk, R.J. *Cyber Incidents Involving Control Systems*; INL/EXT-05-00671; US-CERT Control Systems Security Center: Idaho Falls, ID, USA, 2005.
111. De Cerchio, R.; Riley, C. Aircraft Systems Cyber Security. In Proceedings of IEEE 30th Digital Avionics Systems Conference (DASC), Seattle, WA, USA, 16–20 October 2011.
112. Storey, D. Securing process control networks. *Netw. Secur.* **2009**, *10*, 10–13.
113. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S. Experimental Security Analysis of a Modern Automobile. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
114. Schoitsch, E. Cyber-Physical Systems—What Can We Learn from Disasters with Respect to Assessment, Evaluation and Certification/Qualification of Systems-of-Systems? In Proceedings of 20th IDIMT Conference, Jindrichuv Hradec, Czech Republic, 12–14 September 2012; pp. 69–81.
115. Shachtman, N. Computer Virus Hits U.S. Drone Fleet. *Wired*, 7 October 2011.
116. Cole, C. The Drone War Briefing; Drone Wars UK: Oxford, UK, 2012.
117. Kim, A.; Wampler, B.; Goppert, J.; Hwang, I.; Aldridge, H. *Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles*; The American Institute of Aeronautics and Astronautics: Reston, VA, USA, 2012.

118. Javaid, A.Y.; Sun, W.; Devabhaktuni, V.K.; Alam, M. Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. In Proceedings of IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 585–590.
119. U.S. Government Accountability Office (GAO). *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Aispace System*; GAO-12-981, GAO: Washington, DC, USA, 2012.
120. Loukas, G.; Timotheou, S.; Gelenbe, E. Robotic Wireless Network Connection of Civilians for Emergency Response Operations. In Proceedings of the 23rd International Symposium on Computer and Information Systems (IEEE ISCIS), Istanbul, Turkey, 27–29 October 2008.
121. Kohno, T. Security for Cyber-Physical Systems: Case Studies with Medical Devices, Robots, and Automobiles. In Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC), Tucson, AZ, USA, 16–18 April 2012.
122. Jakobson, G. Mission Cyber Security Situation Assessment Using Impact Dependency Graphs. In Proceedings of the 14th International Conference on Information Fusion, Chicago, IL, USA, 5–8 July 2011.
123. Tadda, G.P.; Salerno, J. Overview of Cyber Situation Awareness. In *Cyber Situational Awareness*; Jajodia, S., Liu, P., Swarup, V., Wang, C., Eds.; Springer: Berlin, Germany, 2010; Volume 46, pp. 15–35.
124. Clem, A.; Galwankar, S.; Buck, G. Health implications of cyber-terrorism. *Prehospital Disaster Med.* **2003**, *18*, 272–275.
125. Halperin, D.; Heydt-Benjamin, T.S.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA, USA, 18–22 May 2008; pp. 129–142.
126. Belala, T.; Issa, O.; Gregoire, J.-C.; Wong, J. A secure mobile multimedia system to assist emergency response teams. *Telemed. e-Health* **2008**, *14*, 560–569.