Chapter 10
TerrorWatch:
A Prototype Mobile App to Combat Terror in Terror-Prone Nations

Solomon Sunday Oyelere
University of Eastern Finland, Finland

Olayemi Olawumi
University of Eastern Finland, Finland

Donald Douglas Atsa'am
Eastern Mediterranean University, Cyprus

Jarkko Suhonen
University of Eastern Finland, Finland

Mike Joy
University of Warwick, UK

Hope Micah Ayuba
Modibbo Adama University of Technology, Nigeria

ABSTRACT

Activities of prominent terrorist groups like Boko Haram, Al-Shabaab, Ansaru, and Ansar Dine have left thousands of people dead and properties destroyed for a number of decades in some developing nations. The high level of insecurity occasioned by operations of terror groups has impacted negatively on the socio-economic development of these nations. On the other hand, the use of mobile devices, such as cell phones, has gained prominence in developing nations over the past two decades. Putting side-by-side these two facts, namely, that the menace of terrorism among some developing nations is alarming and that the use of mobile devices is common among citizens of developing countries, this chapter develops a mobile application prototype called TerrorWatch. TerrorWatch is equipped with relevant menus, buttons, and interfaces that will guide a user on what to do when confronted with a terrorist attack or threat. The unified modeling language (UML) was deployed to design the architecture of the application, while the object-oriented paradigm served in the implementation.

DOI: 10.4018/978-1-5225-4029-8.ch010

INTRODUCTION

The level of insecurity bedeviling most developing nations is alarming (Kim and Phil, 2009). A major cause of this insecurity is terrorism. This has, no doubt, affected this category of nations socio-economically as investors tend to avoid doing business in violent-prone environments. One reassuring fact is that citizens of developing nations have embraced the use of mobile devices. Against this backdrop, the authors are poised to finding a solution to the prevailing problem of terrorism, cashing in on the impressive level of mobile device usage among citizens.

This chapter discusses the design and development of an Android mobile application prototype, called *TerrorWatch,* for developing countries. The application will help users recognize terrorist threats, organizational structures commonly used by terrorist organizations, as well as enable citizens to know when there is imminent danger of an impending terrorist attack. The application provides functionalities that serve as a reference guide to the appropriate line of action when confronted with any form of terrorist threats and/or attack. The application also allows users to warn of an escalating situation to security agents, caution other citizens to steer clear and so forth, using predefined interfaces provided by the application.

According to Whittaker (2004), the primary aim of terrorists is to intimidate the government and society through the use of violence in order to achieve some set goals. In most cases, these goals are political in nature. Terrorist organizations have been ravaging both developed and developing societies for decades. In developing countries, for instance, Boko Haram has been terrorizing Nigeria and Cameroun since 2009, while Al-Shabaab has been operating in Somalia and other East African countries for more than a decade (Wosu and Agwanwo, 2014). The activities of these and many other terrorist groups have posed serious national and regional security and economic challenges. These activities include suicide bombings, hostage-taking, sabotage, high-profile assassinations, indiscriminate and wanton destruction of public and private property, and many more. Huge budgetary allocations, that otherwise would have been channeled to economic development, are made yearly for purposes of war against insurgency. In Nigeria for instance, the year 2014 budget estimates indicated a total of N968.127 billion (nine hundred and sixty eight billion Naira, equivalent to USD 3.2 billion) was earmarked for security (Udo, 2014), and took up 20% of the entire budget for that year. By the year 2016, the budget for security purposes increased to N1.014 trillion (one trillion Naira, equivalent to USD 3.3 billion).

In another development, it is a fact that the use of mobile devices, such as cell phones, has gained prominence in developing nations over the past two decades. In Nigeria, for instance, it is almost impossible to find a household without at least one mobile phone (Oyelere, Suhonen, & Sutinen, 2016). With that in mind, this

research develops an application that will incorporate security features into mobile devices to serve as a counter-measure to the menace of terrorism. Admittedly, there have been concerted efforts by various national and regional security formations to combat terrorism (Cooke, 2013). This, however, has not sufficiently quelled the menace of insurgency, and motivates the authors; to search wider for solutions through the use of mobile devices.

TerrorWatch is a tool to be used by those who require an instant and immediate guide on terrorism and terrorist threats. The application complements, but does not replace, security agents and intelligence gathering on terrorism. Rather, it is an instant solution in the absence of the Army, Police and other relevant agencies. A typical scenario of when the application could be of assistance includes sighting a bomb, firearms, or an improvised explosive device (IED) in an environment, being in a place where attack is taking place, when a terrorist is living around your neighborhood, and when terrorist groups are invading your environment, etc. The application will guide its users on the appropriate action to take in such scenarios.

Given the fact that terrorism is relatively new in most developing countries like Somalia, Nigeria, Cameroon, Mali, and the Niger Republic (McGregor, 2013), most citizens are yet to understand the practical details of this societal ill. The year 2012 saw remarkable terror incidents taking place in Africa, including the Tuareg Ansar al-Din movement that overran northern Mali (McGregor, 2013), the emergence of a new terror faction, Ansaru, from Boko Haram (Zenn, 2012), and an alliance among rebel forces that launched an offensive in the north of the Central Africa Republic (McGregor, 2013). Victims are always helpless in the event of an attack. The populace is frequently confused due to widely divergent views on how to define terrorism. Most persons do not understand the nature of terrorism and do not recognize terrorists and terrorist threats. The *TerrorWatch* application is designed specifically to address these challenges. Admittedly, several applications exist (Mukherjee, 2015; Chrisafis, 2016) for purposes of counter-terrorism. The worrisome issue is that majority of them were designed specifically for the developed world. It is not clear if such applications have options to be customized to fit the terrorism trends in developing countries (Leadbeater, 2015).

TerrorWatch is equipped with relevant menus, buttons, and Graphical User Interfaces (GUIs) that will help a user to call or message the Army, Police or other security agents, quickly, when confronted with a situation that seems to be a terrorist attack or threat. When a user is in a confused situation, as in whether such a situation has any resemblance of terrorism, the application will be useful for clarification. The functionalities of the application certainly will help to save lives and property that otherwise, would have been lost due to terrorism.

The Unified Modeling Language (UML) is deployed to design the architecture of the application (Atsa'am, 2016), while the Android Studio platform and Java served

in the implementation of the application, which can be deployed on any device running the Android operating system. To achieve the design and development of this application, first the functional requirements of *TerrroWatch* are analyzed. Second, the technical architecture as well as implementation details is introduced. Finally, test cases of how the application is used in real-life scenarios are shown, and a formative evaluation plan on how the application will be evaluated is introduced.

BACKGROUND

Relevance of Mobile Devices in Developing Countries

Similar to the developed world, the developing world is not left out in the use of mobile technology. This position is supported by a survey conducted by Oyelere et al (2016) in Nigeria on mobile device ownership among primary and secondary schools students. It was discovered that 54% of the respondents own mobile phones, 17% own smart phones while 10% of the respondents own tablets; 0% own a pocket PC while 1% own an e-Reader; 6% own MP3 players, and the remaining 12% own no mobile devices. This goes to show that among the study participants, 88% of primary and secondary school students in Nigeria own at least a mobile device of one form or another.

Possessing a mobile device is one thing, the use for which the mobile device is put to is another. Salim and Wangusi (2014) presented the possibility of using mobile devices to checkmate corruption in the Water Services sector of Kenya. Research conducted revealed that most Water Service Providers (WSPs) in Kenya are so dubious to the extent that they do not render to water consumers the desired services paid for. Among other integrity deficits, some WSPs are known for supplying unhygienic water to consumers, charging higher rates than the government approved rates, and zero supply for long periods. To solve this situation, Salim and Wangusi (2014) proposed a solution whereby mobile phones would be used to enable consumers provide feedback, escalate corrupt tendencies of WSPs and communicate their satisfaction or dissatisfaction through portals that are monitored by regulatory agencies. A total of 896 Kenya citizens were interviewed to find out from them their preferred method of forwarding complaints to government regarding WSPs. Among the participants, 51% opted for SMS (Short Message Service) platforms, 35% indicated preference for phone calls, while 6% chose social media as their preferred means to disseminate information on water services issues. Premised on this finding, Salim and Wangusi (2014) designed a framework that would employ use of mobile technology to ensure good governance, accountability and satisfaction within the water services sector in Kenya.

Mobile technology could also be harnessed in the area of electronic governance among developing countries. Mukonza (2013) emphasized this through a research conducted in Polokwane Municipality in South Africa. The research revealed that 78% of respondents interviewed had access to the Internet through their mobile devices in urban areas. This percentage is impressive especially coming from a developing country. The worrisome issue however arose when only 4% of the respondents indicated that they do make use of the Internet on their devices to access announcements from the government, make suggestions to government or participate in any form of governmental affairs. This is further compounded by the discovery that many municipalities in South Africa do not own a website in the first place. Even for those that own a website, their citizens are largely unaware of the existence of such. As a result, it is impossible for citizens to follow up with governmental policies and programs electronically. The research held that Polokwane Municipality in South Africa that was used as a case study has a good number of citizens with mobile devices that have access to the Internet. Therefore, it is needful for local governments to take advantage of the situation and facilitate public participation in government through mobile governance.

Oyelere et al (2016) proposed a platform for mobile learning (M-learning) in Nigeria. The research was premised on the high percentage of ownership of mobile devices among primary and secondary school students. When implemented, the students will be able to learn ICT subjects with their cell phones, tablets, and smart phones on the cloud. Teachers could post lessons and homework online for students while at the same time, interacting with students real-time. This no doubt, has the advantage of availing students the opportunity to learn at their convenience, including on the go, using their hand-held devices.

Insight on Terrorism

There is no universally acceptable definition of the term *terrorism*. Divergent views exist on the subject and as such, any definition given is strictly based on context. Whittaker (2004) views terrorism as an act of engaging in violent tendencies to cause coercion or intimidation to a government or the general citizenry. In another assertion, Gupta (2006) describes terrorism as a violent way of passing across a message by a terror group to their enemies for daring to ignore their demands. Dolnik (2007) on the other hand opines that terrorism is an action that employs threat or violence to achieve political gains, be it by a group or an individual. The definition proposed by Dolnik (2007) is adopted when referring to *terrorism* in this chapter.

In as much as the views about terrorism are divergent, they seem to converge at one thing, namely the use of violence. The overall intention of any terrorist group is to terrify the government, citizens or both in order to achieve their objectives. It

is the view of Nance (2008) that some actions by individuals or group may indeed instill fear or terrify the populace but are actually not terrorism. These include incidents like vandalism, armed robbery or murder. Provided such actions are not specifically aimed at terrorizing citizens for the objective of causing a change in government policy, they do not fit the definition of terrorism.

Various methods are employed by terrorist groups to perpetrate violence. Dolnik (2007) listed these to include use of firearms, hostage taking, sabotage, bombings, and suicide bombings. Others include use of chemical, biological, radiological and nuclear agents. Nance (2008) on the other hand enumerates terrorist operations to include assassination, arson, skyjacking, bombing, and abduction.

On why some individuals engage in terrorism, Krueger (2007) at one extreme is of the opinion that marginalization from the economy as well as inability to access education make people feel resentful and consequently resort to terrorism. Nance (2008) at the other extreme holds that some groups engage in terrorism for sole reasons of gaining attention and drawing support for their platform, which may be politically or religiously inclined. Coll et al (2005) attributes the reason some individuals or group resort to acts of terrorism as simply an attempt to gain a distinct identity and for adventure. He pointed out an instance when an adherent of al-Qaeda once said he intended to move to Afghanistan to enroll in the group because of his conviction that it would be a worthwhile adventure. Irrespective of the fact that he was trained as a chef, he was convinced that he would be more fulfilled as a terrorist.

Prominent Terrorist Groups

As part of attempts to sustain the fight against terrorism, the United Nations (UN) through the UN Security Council, maintains a list of groups and entities (United Nations Security Council Subsidiary Organs, 2017) that have been proscribed as terrorists groups by the United Nations. This list, as at 9th December, 2017 is presented in Table 1 in the Appendix. Similarly, the United States through the Secretary of State occasionally designates prominent terrorist groups as Foreign Terrorist Organizations (FTOs) and have the list published (U.S. Department of State, n.d). An incomprehensive list of FTOs as at 3rd March, 2017 is presented in Table 2 in the Appendix.

It is clear from Table 1 and Table 2 that developing countries equally have their fair share of terrorism. It could be observed that a good number of terrorist organizations come from Africa and Asia where there are good numbers of developing nations.

Categories and Common Features of Terrorist Groups

Nance (2008) categorizes terrorist groups according to the geographic area of their operations. Membership of each of these categories is highly dynamic as a group could switch to any other category at any point in time.

- **Local Terrorists:** This category consists of terrorist organizations or individuals operating just within a village, town or city.
- **Regional Terrorists:** The operations of the terrorists cut across a number of cities, states or regions within the borders of a country. For example Ansaru, a breakaway faction of Boko Haram, operating within the North Eastern part of Nigeria (Zenn, 2013).
- **National Terrorists:** The operations of the terrorists encompass most of, if not all, the states or regions within the borders of a country.
- **Transnational Terrorists:** This group of terrorists carries out operations across one or more national boundaries. For example, Boko Haram carries out operations in Nigeria, Cameroon, and the Niger Republic. Another example is Al-Shabaab which operates across the borders of East African countries like Somalia and Kenya.
- **International Terrorists:** This includes those terrorist groups operating in several countries of the world. A prominent example is al-Qaeda.

Apart from the categorization by Nance (2008), Zalman (2017) advances another dimension to types of terrorism. While the former is premised on geographical location, the latter according to Zalman (2017) is based on the motive and means of attack adopted by terrorists.

- **State Terrorism:** This is carried out by a State on her citizens for purposes of achieving political goals (Zalman, 2017). The Nazi rule in Germany, as well as the sponsorship of Hizballah by Iran to actualize her foreign policy objectives have been identified by Zalman (2017) as examples of State terrorism. In same vein, the sponsorship of Nicaraguan Contras by the United States in the 1980s has been argued to be the international dimension to State terrorism (Zalman, 2017). In general, the purpose of this type of terrorism is to force citizens (Blakeley, 2012) into submitting to the dictates of elites.
- **Bioterrorism:** This refers to the premeditated release of harmful living organisms, such as viruses and bacteria, to harm humans, plants or animals with intent to advance a cause (Zalman, 2017). Once introduced into the environment, these biological agents cause fatal damage (Mahendra et al,

2017) that includes death of humans, food poisoning, destruction of plants and animals, and poisoning of oxygen.

- **Eco-Terrorism:** This form of terrorism, according to Zalman (2017), involves use of violence to achieve environmentalism. To facilitate this, extremists engage in sustained attacks on property (and lives in some cases) in order to sabotage industrial activities that cause damage to the environment (Cooke, 2013). Terrorists under this category usually feel the exploration and exploitation activities of companies harm the natural environment and therefore, must be compensated for, or discontinued.
- **Cyber-Terrorism:** This type of terrorism uses information technology to terrorize citizens for purposes of getting attention in a cause (Zalman, 2017). This is achieved, for instance, through abruptly shutting down network connections or computer servers for critical services. Other means might include hacking into public websites and control systems to disrupt or corrupt critical information (Bogdanoski, 2013).
- **Nuclear Terrorism:** Zalman (2017) defines this as the use of nuclear equipment to facilitate terror. This might be done through attack on facilities related to nuclear technology, design and development of nuclear weapons, or the use of radioactive substances to cause havoc and create panic in the society (O'Neill, 1997).
- **Narco-Terrorism:** This was coined in 1983 (Zalman, 2017) and refers to the use of violence by drug peddlers to intimidate and dissuade governments from stopping drug trafficking. Most recently, this form of terrorism is considered to mean the use of illegal drug business by terrorist organizations as a means of raising funds to finance other terror operations (Bjornehed, 2004).

Common Features of Terrorist Groups

As divergent as terrorist groups may appear, they nevertheless have some things in common. Nance (2008) presents eight common characteristics that are inherent in all terrorist organizations.

- **Violence-Prone:** All terrorist groups have a disposition to the use of violence or threat of violence to pass across their message. Different means of perpetrating violence are at their disposal, such as bombs, firearms, IEDs, etc.
- **Environment-Independent:** Terrorist groups have no specific kind of environment within which to operate. They could carry out attacks in churches, mosques, markets, schools and so on. In addition, terrorists operate both in urban or rural areas.

- **Secrecy:** Generally, terrorists operate secretly. Though in some few cases some terror groups may issue advance warnings of their planned attacks, the intention is simply to garner attention of the media and possibly inculcate fear into the populace.
- **Organized Structure:** Terrorist groups usually have an organized structure with a hierarchy that ranges from senior leadership to passive supporters. Boko Haram, for instance, has Abubakar Shekau as the supreme leader. Below him are commanders, field commanders, fighters, active supporters, and passive supporters.
- **Deliberate Action:** Terrorist actions are never random. Any act undertaken by terror groups is well planned before execution. Their attacks are well sequenced and coordinated.
- **Use of Automobiles:** Terrorist groups use means of mobility such as motorcycles and cars to get to areas of operation and back. It is very unlikely for terrorists to get to a target area by foot, unless that is the best method that could enable them get access to a gathering of people in order to execute an attack.
- **Proportionate Weaponry:** Terrorists carefully select the caliber of weapons to employ for any given operation based on need. If the purpose is to assassinate an unarmed individual, for instance, they make use of a small pistol. When a bomb is to be used, the kind of bomb selected for detonation is proportionate to the amount of havoc intended.
- **Media Attention:** Terrorist groups are constantly seeking attention of the media. They often use the media to inculcate fear into citizens and government and also as a channel to make known a cause.

Review of Existing Work on Anti-Terrorism Applications

Mobile devices have been used extensively in both developing and developed nations for communication purposes (such as emailing, text-chatting, sharing of pictures and videos, voice calls, etc), playing games, and several other uses (Mukherjee, 2015). In addition to these uses, many apps have been developed to enable mobile devices function as means to track suspected terrorists and threats. Several such apps are considered in this review.

- **TerrorView:** According to Mukherjee (2015), a company ConteGoView Inc., developed TerrorView, an app capable of synergizing with intelligence experts to gather and manipulate data from as many as 100,000 sources. Having analyzed the accumulated data, the app then alerts users of any

impending terror, biological or cyber-attack within their neighborhood. This provides the user with necessary information needed to steer clear of potential danger zones.

- **FlexiSpy:** This software runs on cell phones and has the capacity to intercept an incoming or outgoing call for Android, iPhone or Blackberry (Mukherjee, 2015). FlexiSpy is able to track Global Positioning System (GPS) location which makes it possible to monitor the location of an individual. The details are compiled and presented as reports for further analysis, which could assist in counter-terrorism.
- **mSpy:** This application can run on almost all hand-held devices (Mukherjee, 2015). With mSpy, text messages on the phone of an individual can be tracked and read. Given this functionality, it is possible to uncover and escalate a plot to unleash terror attack.
- **Saip (Système d'alerte et d'information des populations):** This smartphone app was launched by the French government (Chrisafis, 2016). It is available in both English and French and has the ability to disseminate warnings to individuals; phones when shootings, bombings and other forms of attack occur around their environments. If an attack takes place near a user, the screen background turns red and displays "ALERT", in addition to a brief precautionary measure users must take to ensure their safety.
- **PowerSpy:** This technique is premised on a research finding that power consumption of a phone over time can reveal the user's location (Mukherjee, 2015). The technology is based on the reality that cellular transmissions of a smartphone consume more power as the distance from a cell mast increases, or when obstructed by things such as mountains or buildings. If the software is installed on a phone, it can locate the position of a user, real time, with very high accuracy.
- **LOCINT (Location Intelligence):** This is not actually a mobile application; however it operates in conjunction with mobile devices. If the software is installed on a system, anytime there is detection of a mobile device within a marked out territory, an alert message is sent automatically to a host system (Mukherjee, 2015). With this technology, cell phones can be tracked within a vicinity of 50 meters. Now, if a terrorist is carrying a mobile phone and their number is known, they could be tracked. It is also possible for authorities to rely on this technology to cut off communication channels among terrorists in the process of planning an attack.
- **Highster Mobile:** This software enables a cell phone to be secretly monitored. It spies on inbound and outbound text messages on the phone under scrutiny

and sends gathered information to an Online User Control Panel for prompt review (Mukherjee, 2015). It operates with GPS location tracking to monitor and update the location of a monitored phone within intervals of 10 seconds. With Highster Mobile, terror suspects can be tracked and apprehended provided their mobile numbers are known.

Curiously, all the reviewed mobile applications for counter-terrorism are largely centered on monitoring of terror suspects and tracking their movements. Attention is not given to a functionality that enables users to quickly alert other citizens to keep away from particular environments where a terror attack just occurred or is about to occur. There is no feature in any of the applications that contains images of high-profile terror suspects on the wanted list of security agents. There is equally no functionality that enables users to quickly message or call security agents in instances when a high-profile terror suspect is sighted within vicinity. These gaps need to be addressed.

ANALYSIS, DESIGN, AND IMPLEMENTATION OF *TERRORWATCH*

Analysis of Related Mobile Applications

The mobile applications earlier reviewed have good features, jointly, that are useful in counter-terrorism. Nevertheless, a number of loopholes have been identified among them which make a new application desirable. For instance, applications such as TerrorView, FlexiSpy, PowerSpy, LOCINT, and Highster Mobile presented by Mukherjee (2015) have the following shortcomings inherent in them.

- They are only concerned about tracking the movement, communication and location of terror suspects.
- It is reasonable to infer that they were implemented solely for the developed countries, using terror groups that likely have different ideologies and mode of operation from, for example, Boko Haram, Ansru, Ansar Dine, and Al-Shabaab, which operate in developing countries.
- None of these applications has functionality that a user can query to get guidance when in a confused situation that takes the semblance of terrorism.
- The apps do not have GUIs that display images of terrorists on wanted list, to enable users quickly make comparison and alert security agents if any of such terror suspects is sighted within the environment.

Another app named Saip, presented by Chrisafis (2016) has the capability to alert users and guide them on appropriate cautionary measures to take during a terror attack. However, the application is invoked only when there is a shooting or bombing within the vicinity - Saip is reactive and not proactive. Consider a scenario where a terrorist is sighted conveying IEDs, bombs, etc. Saip has no functionality that can give proper guidance to the user on what to do in such a situation. Given the various shortcomings identified in this analysis, it is imperative that a new app is needed with features that encompass the identified loopholes.

Analysis of the Proposed System

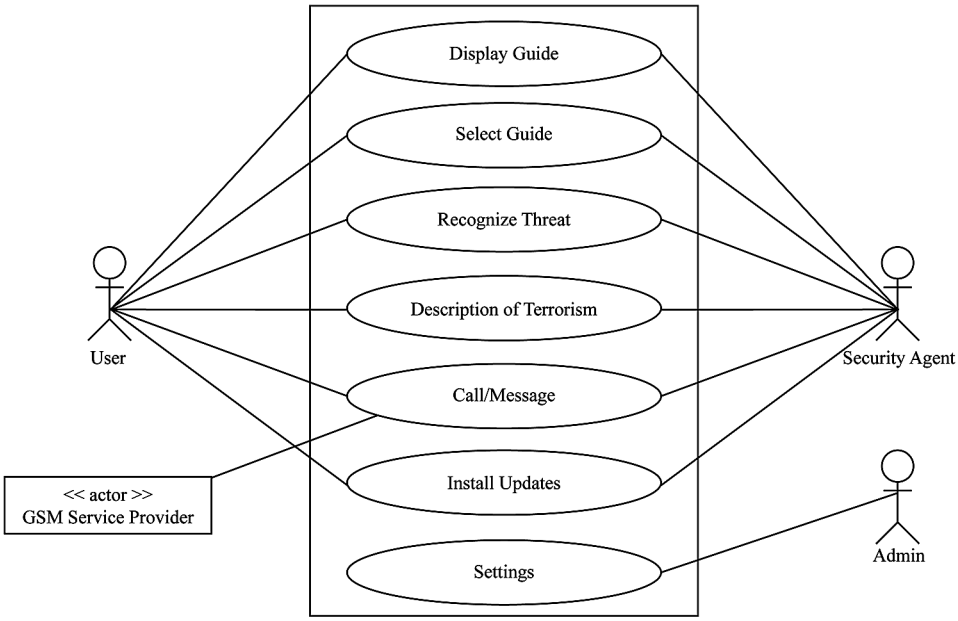
The functionalities that *TerrorWatch* must possess in order to outperform the existing applications are analyzed using Unified Modeling Language (UML). In an application development project, UML enables stakeholders to visualize, specify, document and construct artifacts of the system (Atsa'am, 2016). Several UML tools are at the disposal of developers for use in functional analysis. For purposes of this chapter, the UML use case and activity diagrams are used to analyze the functional requirements of *TerrorWatch*.

Analysis of TerrorWatch With Use Case Diagram

The use case diagrams give graphical descriptions of what functionalities a system has, which actors are involved in using those functionalities, and how those actors and functions interact (Atsa'am, 2016). A functionality of a system is called a *use case.* An *actor* could be a human person, organization or another system that has one or more roles to play in a given system. Four *actors* are identified for the *TerrorWatch* application: *User, Admin, Security Agent, GSM Service Provider*. *User* is any citizen that has the app installed on their mobile device. *Admin*, short for Administrator, is a user with special privileges on the application, such as the ability to update system settings. *Security Agent* refers to the Army, Police, Fire Service, or any government agency with a responsibility in counter-terrorism. The fourth actor, *GSM Service Provider (Telecommunication),* is a different system entirely; however some use cases of *TerrorWatch* must interface with it in order to function. To make calls or send messages with *TerrorWatch*, the services of a GSM provider must be invoked.

Seven use cases are identified in *TerrorWatch* as shown in Figure 1. The *Display Guide* launches the main menu of the application, while the *Select Guide* enables users to choose which menu item they desire. *Call/Message* use case consists of interfaces for users to report terror incidents to *Security Agents* or to caution other users to steer clear of certain zones. For this use case to function, a system actor

Figure 1. Use case diagram of TerrorWatch



namely, *GSM Service Provider,* such as MTN, Globacom, Safaricom, Airtel, and Vodafone, must be involved. The *Recognize Threat* use case consists of pre-defined terror scenario that users can query to get clarification when they find themselves in situations that take semblance of imminent terror threat or attack. This use case also displays images of wanted terror suspects so that when users sight them within an environment, they do due diligence by way of taking proper caution not to be endangered, while at the same time alerting relevant security agents. The *Description of Terrorism* use case is necessary, especially in some developing countries where terrorism is relatively new. Terrorism-related terminologies like abduction, hostage-taking, hijack, bomb, IED, etc, are described and made easy to locate on *TerrorWatch* so users can quickly consult for clarification when the need arises. The *Install Updates* functionality enables users to update the *TerrorWatch* application when a new version, patch or fix is available. This is important because, for example, additional high profile terror suspects may be declared wanted, new terrorism-related terms and techniques may emerge with time, or higher versions of the application could come up with improved technology. The *Settings* use case is accessible to only the *Admin* for purposes of making changes to current system settings, making new versions of the application available for users, and updating system definitions.

Analysis of TerrorWatch With Activity Diagram

According to Miller (2013), UML activity diagrams focus on the flow of events that are needed to achieve some task with a system. An activity diagram is used in this section to show graphically the series of activities that take place when a user sights a wanted terror suspect, bomb, IED, etc, within the environment.

As depicted in Figure 2, when users encounter any form of terror threat within their environment, they quickly launch the mobile app on their phone and at the same time take safety precautions – generally referred to here as *take cover.* They then place a call or send a message containing the details of the threat to other users. If the recipient is the security center, security agents take measures to contain the situation and the process terminates. On the other hand, if the call or message is to civilian users, the users heed the warning and *take cover*, and the process terminates.

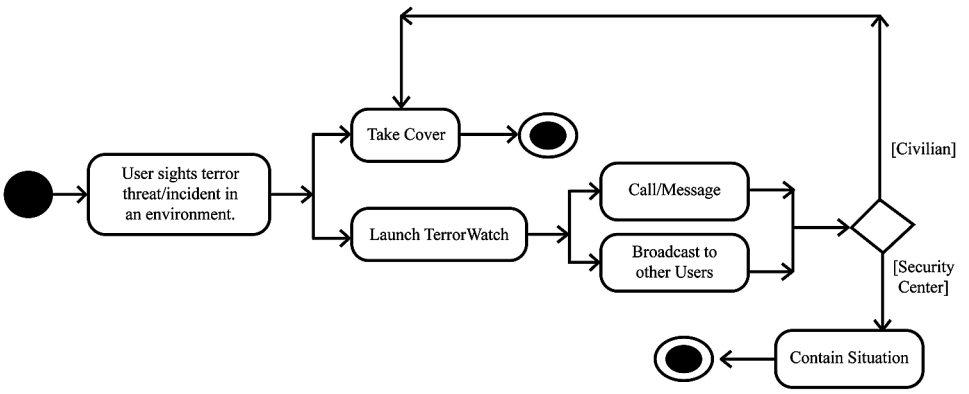
Design of the TerrorWatch Architecture

At this stage, the architectural design of *TerrorWatch* is presented. To achieve this, system requirements earlier specified at the analysis stage are taken into consideration. This is necessary in order to put forth a robust design that meets the objectives for which this app is intended. UML class and sequence diagrams are employed in the design of the application.

Design of TerrorWatch With Class Diagram

A class diagram shows the overview of the structure of a system in terms of its classes and the relationship between those classes (Atsa'am, 2016). Basically, *TerrorWatch*

Figure 2. Activity diagram of TerrorWatch when user sights a terror threat



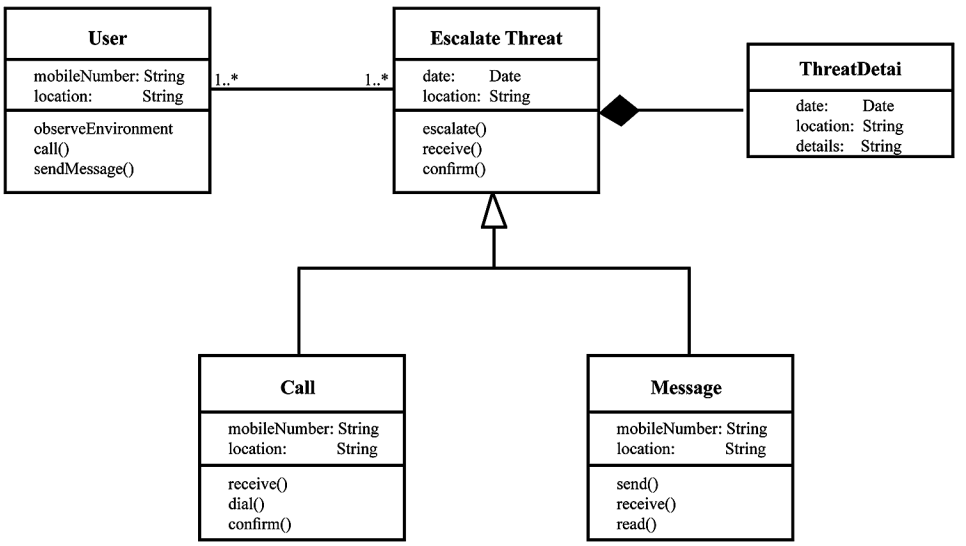
consists of five classes: *User, EscalateThreat, ThreatDetail, Call, and Message.* A class consists of three parts: class name at the top, class attributes in the middle, and the operations associated with the class at the bottom.

Three different types of relationships exist among the five classes of the app as depicted in Figure 3. An *association* relationship exists between the instances of *User* and *EscalateThreat* classes. The instance of *User* class must know about the instance of the *EscalateThreat* class in order to perform a task, and vice-versa. Clearly, this means there is dependency among the classes. The "1..*" at both ends of the association arrow is called *multiplicity*, and it means that one or many *Users* can perform one or many *EscalateThreat* tasks at a time.

A *generalization* relationship, also called inheritance, exists between the *Call* and the *Message* classes on the one hand and the *EscalateThreat* class on the other hand. The *EscalateThreat* class is a superclass in this case. The actual means by which *Threat* instances can be escalated is either through phone *Call* or *Message*, which are subclasses.

The third type of relationship depicted in Figure 3 is a *composition* relationship between the *EscalateThreat* and *ThreatDetail* classes. A *composition* relationship exists between two classes where one class is a "whole" class while the other is a "part" class. In this case, *ThreatDetail* is part of the *EscalateThreat* class, and if the latter is deleted, the former is automatically deleted.

Figure 3. Class diagram of TerrorWatch



Design of TerrorWatch With Sequence Diagram

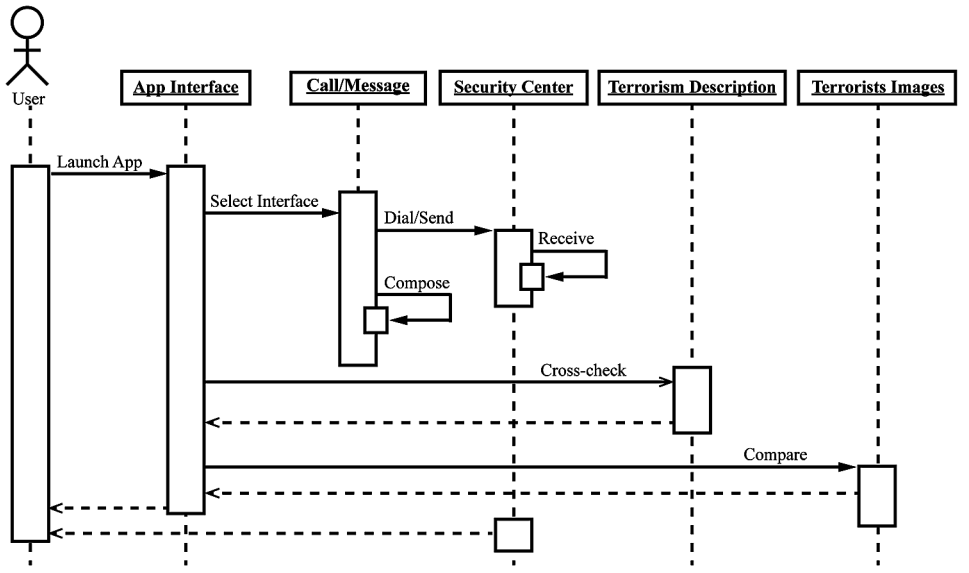
Sequence diagrams enable system designers to illustrate the interaction between users, interfaces, and objects that make up a system (Miller, 2013). With this UML tool, it is easy to show the order of sequence by which messages are passed between objects and entities of a system over time.

Basically, six objects participate in message passing in *TerrorWatch* as observed in Figure 4. The objects include: *User, App Interface, Call/Message, Security Center, Terrorism Description,* and *Terrorists Images.* Two different kinds of arrows are used in the diagram to represent particular form of communication between objects of the app. The full arrows indicate *synchronous* messages, while the dashed arrows are *reply* messages. A message is said to be *synchronous* if, upon sending the message, the sender object suspends execution while waiting for response from the receiver object. A *reply* message, as the name implies, is a feedback from an operation call.

The following sequence of events can be deduced from Figure 4.

- *User* encounters a terror threat or incident within an environment then quickly launches the application. The graphical user interface, *App Interface*, opens. *User* selects the *Call/Message* interface and dials the emergency number, or composes a text message, and sends to the emergency number. The *Security Center* receives the call or message and sends feedback to *User.*

Figure 4. Sequence diagram of TerrorWatch



- *User* encounters a confused situation within the vicinity that seems to be a terror scenario. Among the app interfaces, *User* selects the *Terrorism Description* interface which has pre-defined terrorism terminologies and cases to cross-check against the situation at hand. If the prevailing situation fits the terrorism definition, the *App Interface* is useful next.
- *User* sights a wanted terror suspect within neighborhood. In order to be double sure, they quickly select the interface that has images of terrorists on the wanted list and compares against the person they have seen. If the comparison matches, the *App Interface* is useful next.

The architectural design is transformed into a working system in the next section, using appropriate programming tools.

Implementation

At this stage, the design carried out in the previous section is implemented and transformed into a prototype mobile application. The attributes and methods of each object are implemented and all objects are integrated such that they function as a single system. During this phase, the authors describe how the prototype application is built using object-oriented coding requirements, and also how testing is done to guarantee that it functions properly.

Development Environment

The programming methodology used in implementing *TerrorWatch* is the object-oriented paradigm (OOP). OOP is a programming style that allows a programmer to implement a program as a collection of cooperating objects (Dennis et al, 2006). A number of objects were identified and designed at the design stage. At this point, each of those objects is coded and then integrated with other objects to function as a whole system.

Testing and documentation are carried out hand-in-hand during implementation of the application. To complete program testing, the source codes are executed experimentally to make sure the desired result is achieved. To ensure the effectiveness of the program logic, the debugging feature available in the development tool is used to trace errors and fix them accordingly. Documentation has been done right from the analysis and design stage of the project by use of UML diagrams. At the implementation stage, comments are used to make short notes against source codes that may appear confusing to programmers at later times in the event of program maintenance.

TerrorWatch GUIs

Graphical User Interfaces consisting of icons, menus, buttons, texts, or other visual indicators, which enable users to interact with *TerrorWatch* via mobile devices, are implemented as shown in this section.

When a user launches the application, the main menu appears as shown in Figure 5. The main menu consists of five submenus: *Guide to Terrorism, Recognizing a Threat, Description of Terrorism, Call,* and *Message.*

Upon encountering a terror attack or threat by a user, the *Guide to Terrorism* submenu, shown in Figure 6, is available to provide guidance on the appropriate line of action to take.

Figure 7 shows the submenu a user can quickly consult to determine if an ongoing situation around the environment has any terrorism connotation.

If a user comes across a terror suspect within the neighborhood, the submenu shown in Figure 8 is quickly queried to compare the suspect against the images of terrorists populated in the application. If the comparison is in the affirmative, security agents are immediately notified. The user must, however, do so in a way that their safety is not compromised.

Figure 9 shows the interface where users can place calls to the security center or other users to escalate terror instances.

In order to send messages to the security center and to other users regarding terror incidents, the interface shown in Figure 10 suffices.

Figure 5. Main menu

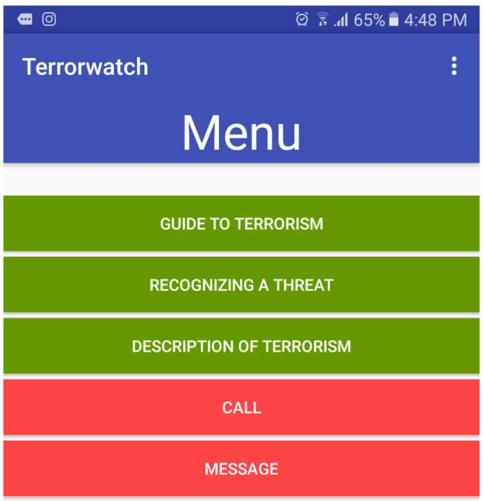
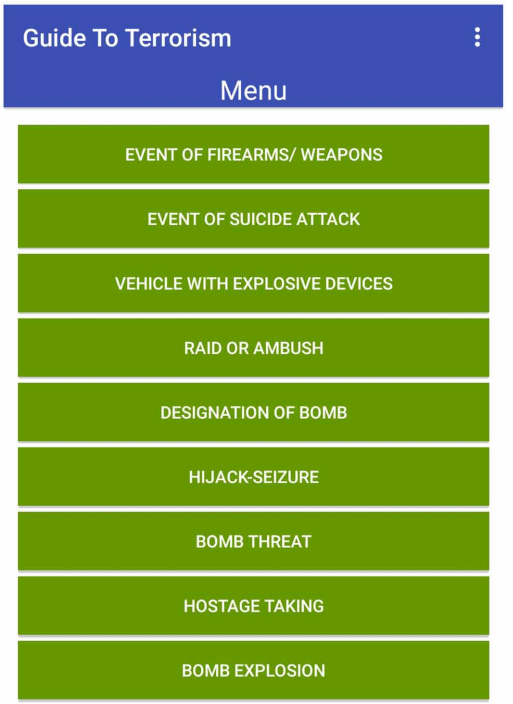


Figure 6. Guide to terrorism



Deployment Platform

TerrorWatch is a mobile application developed to be compatible with all versions of the Android operating system. The hardware must be a tablet, smartphone, or phone of any brand, running the Android operating system. In addition, the mobile devices require a minimum of 512 MB memory of RAM. The fact that *TerrorWatch* requires GSM network to function, the mobile device must be provided with at least one functional Subscriber Identification Module (SIM) card to establish a network connection.

Deployment diagrams, according to Miller (2013), are used in modeling the physical deployment of a system to the production or test environment, detailing the hardware and software requirement. The UML deployment diagram in Figure 11 illustrates how *TerrorWatch* is to be deployed. The TerrorWatch application is sitting on the Android operating system, both of them located in a smartphone.

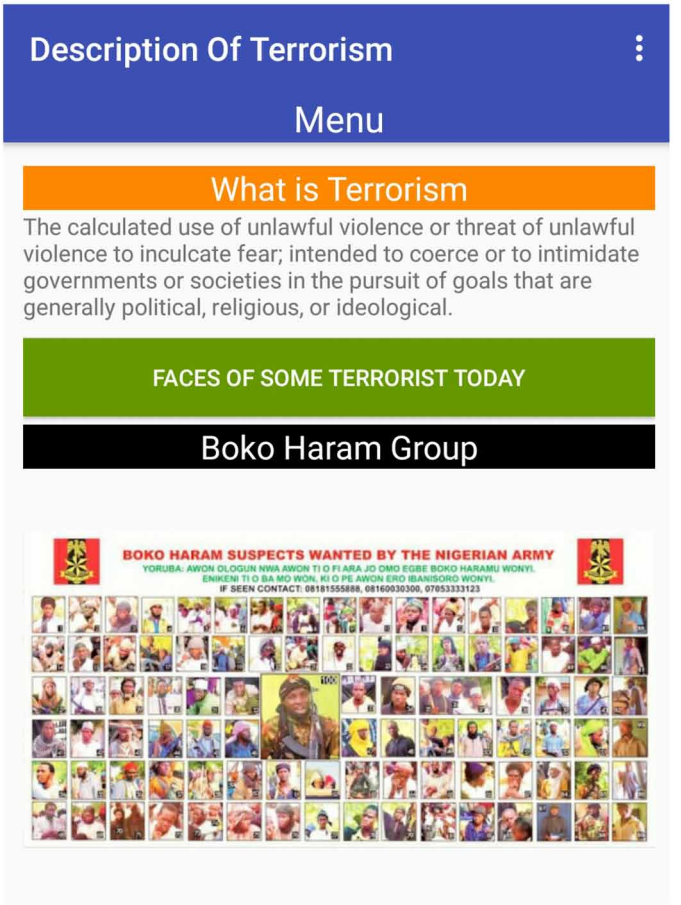
Figure 7. Recognizing a threat

EVALUATION PLAN, EXPECTED SOLUTIONS, AND RECOMMENDATIONS

The next step in the development of the tool is to deploy and evaluate *TerrorWatch* in a real-life setting. Two locations have been identified for the deployment, and they are localities ravaged by Boko Haram in North-East Nigeria: Borno and Adamawa states.

To achieve the evaluation process, the application would be installed on the phones of select individuals, 50 in each state, for test-run. It is intended that during this procedure, the functionalities of *TerrorWatch* are utilized by 100 users, within three months, to determine how well this application meets its design goals. After the three-month duration, feedback will be collected from users to assist in corrective maintenance of the app.

Figure 8. Description of terrorism



When deployed to live usage, it is envisaged that the awareness level of citizens of emerging nations on terrorism-related issues would tremendously improve. This is given the fact that *TerrorWatch* has special features dedicated specifically to enlighten users on what terrorism is all about. Users of the app will have various descriptions of terrorism on their fingertips to quickly consult when in confused situations. The application also has the capacity to curtail the menace of terrorism currently ravaging most developing nations. With the escalation feature, through message or call, potential terror attacks that would otherwise have occurred can be prevented. Even if they do occur, casualty figure would be reduced provided a user gave advance warning on sighting a threat, and other users or security agents in turn heed the warning. *TerrorWatch* is handy to give the needed guidance to citizens on what to do when they find themselves in the midst of a terror threat or attack.

Figure 9. Call interface

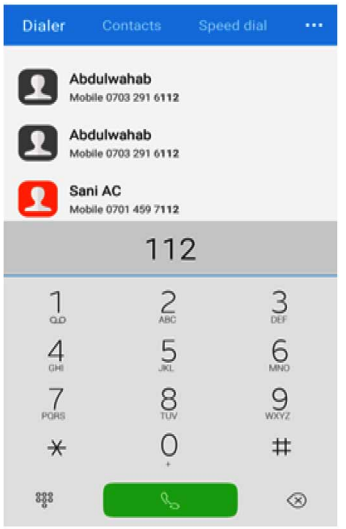


Figure 10. Message interface

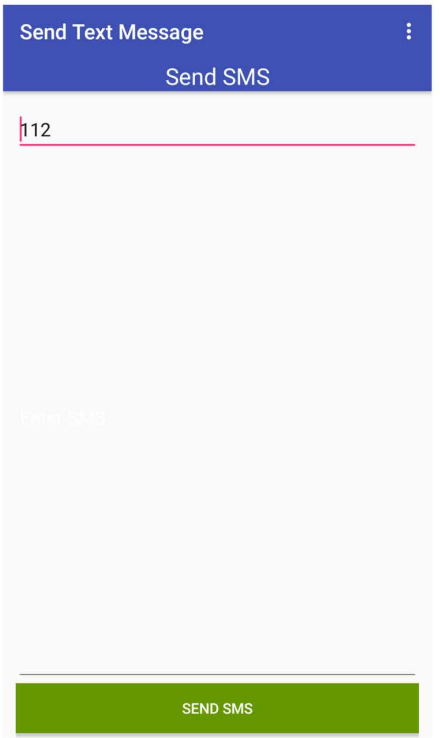
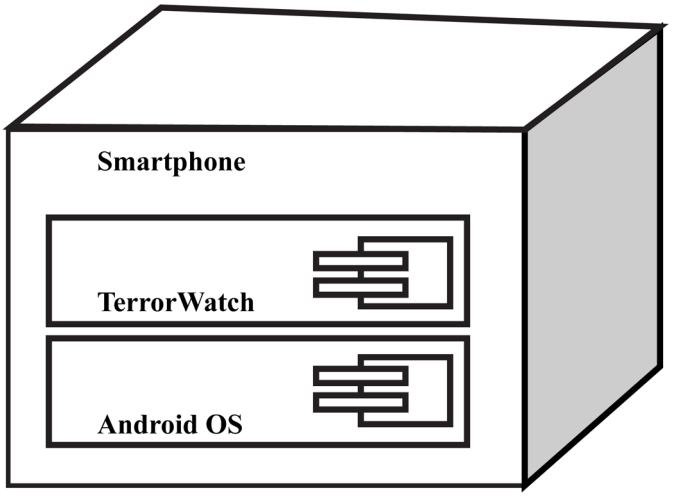


Figure 11. Deployment diagram of TerrorWatch



It is recommended that, as many as possible, citizens of developing nations have a fully developed version of the application installed on their mobile devices. Users should not compromise their personal safety when escalating issues with *TerrorWatch.* Cautionary measures must be taken by users attempting to report terror incidents with the application. Users should ensure that their safety is not sold out to any suspects that might be around them when escalating terror situations.

FUTURE RESEARCH DIRECTIONS

The application developed in this chapter is a prototype. Further work needs to be done in order to put forth an all-encompassing version of *TerrorWatch.* For instance, the menus, buttons and texts that users will make use of while navigating the application are implemented entirely in the English language. It turns out that English is not the only popular language among all the developing countries for which the application is intended. Other languages like French, Arabic, Swahili, Hausa, Yoruba, Ibo, Tiv, Zulu, Shona, and many others, are widely spoken across emerging nations. These have to be put into consideration in subsequent versions of the application.

Aside from the language barrier issue, *TerrorWatch* has no intelligence of its own. It has no capacity to detect bombs, IEDs and other threats automatically. The human user has to initiate an escalation cycle with the application, each time. This has to be equally researched, so that an intelligent version of the application could

emerge. This is necessary due to the fact that an automated system is not erratic or prone to judgmental bias unlike humans.

It might be appropriate to consider developing a version of *TerrorWatch* that is compatible with all forms of mobile phones, not just smart phones. This is premised on the findings by Oyelere et al (2016) which revealed that only 17% of respondents in a survey in Nigeria owned smart phones; while majority owned non-smart phones.

CONCLUSION

Most emerging nations have had their own fair share of terrorism. There can be no reasonable economic development in environments that are insecure. Apart from the high rate of corruption and inadequate technology, many developing countries are backward economically as a result of insecurity associated with them. It is natural for investors to avoid doing business in countries where terrorism holds sway. The reassuring side is that emerging nations have embraced the use of mobile devices and associated technologies, which are what *TerrorWatch* needs to function. It is envisaged that with this application, terrorism will be reduced reasonably, thereby rendering the environments conducive for economic activities. Huge budgetary spending on security would equally be directed towards more productive sectors of the economy. All thanks to mobile technologies.

REFERENCES

Atsa'am, D. (2016). *A practical guide to using UML tools in system analysis and design*. Saarbrucken, Germany: Lambert Academic Publishing.

Bjornehed, E. (2004). Narco-Terrorism: The Merger of the war on drugs and the war on terror. *Global Crime*, *6*(3&4), 305–324. doi:10.1080/17440570500273440

Blakeley, R. (2012). State violence as state terrorism. In M. Breen-Smyth (Ed.), *The Ashgate research companion to political violence* (pp. 63–78). Farnham, UK: Ashgate Publishing.

Bogdanoski, M. (2013). Cyber terrorism – global security threat: Contemporary macedonian defence. *International Scientific Defence, Security and Peace Journal*, *13*, 59-72.

Chrisafis, A. (2016). *France launches smartphone app to alert people to terror attacks.* Retrieved March 26, 2017, from https://www.theguardian.com/world/2016/jun/08/france-smartphone-app-alert-terror-attacks-saip

Coll, S., Fouda, Y., Stern, J., & Sageman, M. (2005). Who joins al Qaeda. In K. J. Greenberg (Ed.), *Al Qaeda now* (pp. 27–41). Cambridge, UK: Cambridge University Press. doi:10.1017/CBO9780511510489.005

Cooke, S. (2013). Animal rights and the environment. *Journal of Terrorism Research*, *4*(2), 26–36. doi:10.15664/jtr.532

Dennis, A., Wixom, B., & Roth, R. (2006). *Systems analysis and design* (3rd ed.). John Wiley & Sons, Inc.

Dolnik, A. (2007). *Understanding terrorist innovation technology, tactics and global trends*. New York, NY: Routledge. doi:10.4324/9780203088944

Gupta, D. K. (2006). *Who are the terrorists?* San Diego State University: Chelsea House Publishers.

Kim, T., & Phil, D. (2009). *The sources of insecurity in the third world: external or internal? Shinjuku-ku*. Tokyo: Waseda Institute for Advanced Study.

Krueger, A. B. (2007). *What makes a terrorist: economies and roots of terrorism*. Princeton, NJ: Princeton University Press.

Leadbeater, C. (2015). *New app could alert travellers about terror attacks.* Retrieved March 26, 2017, from http://www.telegraph.co.uk/travel/news/New-app-could-alert-travellers-about-terror-attacks/

Mahendra, P., Meron, T., Fikru, G., Hailegebrael, B., Vikram, G. & Venkataramana, K. (2017). An overview of biological weapons and bioterrorism. *American Journal of Biomedical Research, 5*(2), 24-34.

McGregor, A. (2013). Islamist groups mount joint offensive in Mali. *Terrorism Monitor, In-Depth Analysis of the War on Terror*, *XI*(1), 1–3.

Miller, R. (2003). *Practical UML: A hands-on introduction for developers.* Retrieved April 21, 2017, from http://edn.embarcadero.com/article/31863

Mukherjee, S. (2015). *Counter-terrorism in your pocket: Smartphone apps that make you feel safer (sometimes).* Retrieved March 26, 2017, from http://www.dnaindia.com/scitech/report-now-apps-can-help-you-fight-terrorism-2149233

Mukonza, R. M. (2013). M-government in South Africa's local government: A missed opportunity to enhance public participation? In *Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance* (vol. ICEGOV'13, pp. 374-375). New York: ACM. doi:10.1145/2591888.2591966

Nance, M. W. (2008). *Terrorist recognition handbook: a practitioner's manual for predicting and identifying terrorist activities* (2nd ed.). CRC Press. doi:10.1201/9781420071849

O'Neill, K. (1997). *The nuclear terrorist threat.* Retrieved December 8, 2017, from http://www.isis-online.org/publications/terrorism/threat.pdf

Oyelere, S. S., Suhonen, J., & Sutinen, E. (2016). M-learning: A new paradigm of learning ICT in Nigeria. *International Journal of Interactive Mobile Technologies*, *10*(1), 35–44. doi:10.3991/ijim.v10i1.4872

Salim, A., & Wangusi, N. (2014). Mobile phone technology: An effective tool to fight corruption in Kenya. In *Proceedings of 15th Annual International Conference on Digital Government Research* (pp. 300-305). New York: ACM.

Udo, B. (2014). *Jonathan signs Nigeria's 2014 budget as defence gets 20 per cent.* Retrieved March 26, 2017, from http://www.premiumtimesng.com/business/161390-jonathan-signs-nigerias-2014-budget-defence-gets-20-per-cent.html

United Nations Security Council Subsidiary Organs. (2017). *Sanctions list materials.* Retrieved December 9, 2017, from https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida.xsl

U.S. Department of State. (n.d.). *Foreign terrorist organizations.* Retrieved March 3, 2017, from https://www.state.gov/j/ct/rls/other/des/123085.htm

Whittaker, J. D. (2004). *Terrorists and terrorism in the contemporary world.* London: Routledge.

Wosu, E., & Agwanwo, D. E. (2014). Boko haram insurgency and national security challenges in Nigeria: An analysis of a failed state. *Global Journal of Human-Social Science*, *14*(7), 10–19.

Zalman, A. (2017). *Types of terrorism: A guide to different types of terrorism.* Retrieved December 6, 2017, from https://www.thoughtco.com/types-of-terrorism-3209376

Zenn, J. (2013). Ansaru: A profile of Nigeria's newest jihadist movement. *Terrorism Monitor, In-Depth Analysis of the War on Terror*, *11*(1), 7–9.

KEY TERMS AND DEFINITIONS

Android: An operating system designed mainly to run touchscreen handheld devices such as smartphones and tablets.

Architecture: A model that conceptualizes the structure and behaviour of a system to enable an observer to have an overview of that system.

Graphical User Interface: A medium consisting of icons, menus, buttons, texts, or other visual indicators that enable users to interact with a system.

Mobile Application: Also referred to as app, is software developed to run on devices such as phones, smartphones, and tablets.

Mobile Device: Handheld computing device such as phone, smartphone, or tablet.

Terrorism: The use of violence or threat of violence against civilians or military to achieve political goals.

Unified Modeling Language: A graphical language that provides a way for conceptualizing the design of a system.

APPENDIX: LISTS OF TERRORIST ORGANIZATIONS

The lists of terrorist organizations maintained by the United Nations, on the one hand, and the United States, on the other hand, are presented. Comparison between these lists reveals that similarities exist among them.

Table 1. Terrorist entities and groups

Name	Region	Location of Operations
Abu Sayyaf Group	Asia	Philippines
Al-Itihaad Al-Islamiya / Aiai	Africa	Somalia
Egyptian Islamic Jihad	Africa	Egypt
Al-Qaida		
Al Rashid Trust	Asia	Pakistan
Armed Islamic Group	Africa	Algeria
Asbat Al-Ansar		Lebanon
Harakat Ul-Mujahidin / Hum	Asia	Pakistan
Islamic Army of Aden		Yemen
Islamic Movement of Uzbekistan		Uzbekistan
Libyan Islamic Fighting Group	Africa	Libyan Arab Jamahiriya
Makhtab Al-Khidamat	Asia	Pakistan
The Organization of Al-Qaida In The Islamic Maghreb	Africa	Algeria, Mali, Mauritania, Morocco, Niger, Tunisia
Wafa Humanitarian Organization	Asia, Middle East	Pakistan, Saudi Arabia Kuwait, United Arab Emirates
Jaish-I-Mohammed	Asia	Pakistan
Jam'yah Ta'awun Al-Islamia	Asia	Kandahar City, Afghanistan
Rabita Trust	Asia	Pakistan
Ummah Tameer E-Nau (UTN)	Asia	Afghanistan, Pakistan
Afghan Support Committee (ASC)	Asia	Pakistan, Afghanistan
Revival of Islamic Heritage Society	Asia	Pakistan, Afghanistan
Al-Haramain Islamic Foundation	Europe	Bosnia and Herzegovina
Al-Haramain Islamic Foundation (Somalia)	Africa	Somalia
Eastern Turkistan Islamic Movement (ETIM)	Asia	Turkistan
Moroccan Islamic Combatant Group	Asia, Europe	Afghanistan, United Kingdom, Morocco
Global Relief Foundation (GRF)	America	United States

continued on following page

Table 1. Continued

Name	Region	Location of Operations
Jemaah Islamiyah	Asia	Philippines, Malaysia, Indonesia
Benevolence International Foundation	Africa, Asia, America, Middle East	United States, Sudan, Bangladesh, Yemen, Gaza Strip
Lashkar Jhangvi (LJ)	Asia	Pakistan
Ansar Al-Islam	Middle East	Iraq
Islamic International Brigade (IIB)	Asia, Eurasia	Afghanistan Russia
Special Purpose Islamic Regiment (SPIR)	Eurasia	Russia
Djamat Houmat Daawa Salafia (DHDS)	Africa	Algeria
Al-Haramain Foundation	Asia	Indonesia, Pakistan
Al-Haramayn Foundation	Africa	Kenya, Tanzania
Al Furqan	Europe	Bosnia and Herzegovina
Taibah International-Bosnia Offices	Europe	Bosnia and Herzegovina
Al-Haramain & Al Masjed Al-Aqsa Charity Foundation	Europe	Bosnia and Herzegovina
Al-Haramain: Afghanistan Branch	Asia	Afghanistan
Al-Haramain: Albania Branch	Europe	Albania
Al-Haramain: Bangladesh Branch	Asia	Bangladesh
Al-Haramain: Ethiopia Branch	Africa	Ethiopia
Al-Haramain: The Netherlands Branch	Europe	Netherlands
Al-Qaida In Iraq	Middle East	Iraq, Syria
AL-Haramain Foundation (Union of the Comoros)	Africa	Comoros
Lashkar-E-Tayyiba	Asia	Pakistan
Islamic Jihad Group	Europe, Asia	Uzbekistan, Afghanistan, Germany, Pakistan
Al-Akhtar Trust International	Asia	Pakistan
Rajah solaiman movement	Asia	Philippines
Al-Qaida In The Arabian Peninsula (AQAP)	Middle East	Yemen, Saudi Arabia
Harakat-ul Jihad Islami	Asia	India, Pakistan, Afghanistan
Emarat Kavkaz	Euroasia, Europe, Asia	Russia, Sweden, Afghanistan, Pakistan
Tehrik-E Taliban Pakistan (TTP)	Asia	Pakistan, Afghanistan
Jemmah Anshorut Tauhid (JAT)	Asia	Indonesia
Mouvement Pour L'unification Et Le Jihad en Afrique De L'ouest (MUJAO)		

continued on following page

Table 1. Continued

Name	Region	Location of Operations
Ansar Eddine	Africa	Mali
Muhammad Jamal Network (MJN)	Africa	Egypt, Libya, Mali
Al-Nusrah Front for the People of the Levant	Middle East	Syrian Arab Republic, Iraq
Jama;atu Ahlis Sunna Lidda;awati Wal-Jihad (Boko Haram or Western Education Sinful)	Africa	Nigeria
Al Mouakaoune Biddam	Africa	Mali
Al Moulathamoun	Africa	Mali, Algeria, Niger
Al Mourabitoun	Africa	Mali
Ansarul Muslimina fi Biladis Sudan (Ansaru)	Africa	Nigeria
Ansar Al-Shari;a in Tunisia (AAS-T)	Africa	Tunisia
Abdallah Azzam Brigades (AAB)	Middle East	Lebanon, Syria, Arabian Peninsula
Ansar al Charia Derna	Africa	Libya, Tunisia
Ansar al Charia Benghazi	Africa	Libya, Tunisia
Hilal Ahmar Society Indonesia (HASI)	Asia	Indonesia
The Army of Emigrants and Supporters	Middle East	Syria
Harakat Sham al-Islam	Middle East	Syria
Mujahidin Indonesian Timur (MIT)	Asia	Indonesia
Jund Al-Khilafah in Algeria (JAK-A)	Africa	Algeria
Jamaat-Ul-Ahrar (JUA)	Asia	Afghanistan, Pakistan
Hanifa Money Exchange Office (BRANCH LOCATED IN Albu Kamal, Syrian Arab Republic)	Middle East	Syrian Arab Republic
Selselat Al-Thahab	Middle East	Iraq
Jaysh Khalid Ibn al Waleed	Middle East	Syria
Jund Al Aqsa	Middle East	Syrian Arab Republic

United Nations Security Council Subsidiary Organs, 2017.

Table 2. Foreign terrorist organizations

Name	Region	Location of Operations
Abu Nidal Organization (ANO)	Middle East	Palestinian Territories
Abu Sayyaf Group (ASG)	Asia	Philippines
Communist Party of the Philippines/New People's Army (CPP/NPA)	Asia	Philippines
Jemaah Islamiya organization (JI)	Asia	Indonesia
Lashkar i Jhangvi	Asia	Pakistan
Al-Qaeda Kurdish Battalions	Middle East	Iraq
Continuity Irish Republican Army (CIRA)	Europe	Ireland, United Kingdom
Islamic State of Iraq and the Levant (formerly Al-Qaeda in Iraq aka Tanzim Qa;idat al-Jihad fi Bilad al-Rafidayn (QJBR))	Worldwide	Iraq, Syria, Libya, Nigeria
Islamic Jihad Union (IJU)	Asia	Uzbekistan
Harkat-ul-Jihad al-Islami (HUJI-B)	Asia	Bangladesh
Al-Shabaab	Africa	Somalia
Jundallah (People's Resistance Movement of Iran, or PRMI) (Iran)	Asia	Iran
Army of Islam (Palestinian)	Middle East	Palestinian Territories
Indian Mujahideen (IM) (India)	Asia	India
Jamaah Ansharut Tauhid (JAT)	Asia	Indonesia
Abdullah Azzam Brigades	Middle East	Iraq
Haqqani network	Asia	Afghanistan
Ansar Dine	Africa	Mali
Boko Haram	Africa	Nigeria
Ansaru	Africa	Nigeria
al-Mulathamun Brigade	Africa	Algeria
Ansar al-Shari'a in Benghazi	Africa	Libya
Ansar al-Shari'a in Darnah	Africa	Libya
Ansar al-Shari'a in Tunisia	Africa	Tunisia
Ansar Bayt al-Maqdis	Africa, Middle East	Egypt
Al-Nusra Front	Middle East	Syria
Mujahideen Shura Council in the Environs of Jerusalem	Africa, Middle East	Egypt
Jaysh Rijal al-Tariq al Naqshabandi (JRTN)	Middle East	Iraq
ISIL Khorasan	Asia	Afghanistan
ISIL Libya	Africa	Libya
Al-Qa'ida in the Indian Subcontinent	Asia	India

U.S. Department of State, n.d.