Z E S Z Y T Y N A U K O W E P O L I T E C H N I K I P O Z N A Ń S K I E J
Nr 76 Organizacja i Zarządzanie 2018

Mieczysław OGÓREK*, Piotr ZASKÓRSKI*

INTERNET RZECZY W INTEGRACJI PROCESÓW ZARZĄDZANIA KRYZYSOWEGO

DOI: 10.21008/j.0239-9415.2018.076.15

W artykule przedstawiono zarys koncepcji wykorzystania Internetu rzeczy (Internet of Things – IoT) w procesach zarządzania kryzysowego oraz korzyści, jakie z tego wynikają a także zagrożenia z tym związane. Podjęto przy tym próbę identyfikacji obszaru i dziedzin użycia Internetu rzeczy w szeroko pojmowanych systemach zapewniania bezpieczeństwa. Rozważania podjęte w tym opracowaniu skłaniają ku szerszemu spojrzeniu na problem Internetu rzeczy, podkreślają jego znaczenie i rolę w dynamicznie zmieniającym się świecie, który wraz z rozwojem technicznym i globalizacją narażony jest na coraz to nowsze z tym związane zagrożenia, które wymuszają potrzebę wzmacniania i doskonalenia systemów zarządzania kryzysowego, szczególnie w kontekście zapewniania informacyjnej ciągłości działania.

Słowa kluczowe: Internet rzeczy, (IoT), Internet przedmiotów, zarządzanie kryzysowe, smart city

1. WPROWADZENIE

Postęp technologiczny generuje nowe rozwiązania, ale z drugiej strony generuje także wiele nowych zagrożeń. Szczególnie jest to widoczne w obszarze teleinformatyki i elektroniki. Internet i technologie informacyjne sprzyjają informatyzacji i integracji wielu rozproszonych podmiotów. Dotyczy to zarówno specjalizowanych obiektów, jak i całych miast. Procesy nadzorowania i monitorowania stały się powszechniejsze poprzez coraz nowsze rozwiązania tzw. „inteligentne" urządzenia, czujniki, zaawansowane technologicznie sensory itp. Internet rzeczy staje się więc efektywną platformą integracji usług informacyjnych. Architektura Internetu

* Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Organizacji i Zarządzania.

została zaprojektowana jako narzędzie do komunikacji, ale dziś staje się wszechobecna, interaktywna i coraz to bardziej zaawansowana. Funkcja komunikacyjna związana ściśle z relacjami międzyludzkimi została rozszerzona na komunikowanie się przedmiotów.

W chwili obecnej elementy takie jak sensory, odbiorniki, procesory, smart-urządzenia i ich oprogramowanie coraz częściej stają się nierozerwalną składową szeroko rozumianych produktów (rzeczy). Jednocześnie posiadają same w sobie zdolności łączenia się z zewnętrzną warstwą infrastrukturalną. Możliwości takie powodują swoiste zmiany w ich działaniu i sposobie wykorzystania ich funkcji. Wszystko to daje nowe możliwości nie tylko wzrostu funkcjonalności różnego typu rozwiązań, ale także zapewniania ciągłości działania (Zaskórski P., 2011) i przeciwdziałania sytuacjom kryzysowym na dowolnym szczeblu zarządzania, a w szczególności w szeroko rozumianym obszarze bezpieczeństwa państwa. Internet rzeczy może więc stać się integralnym elementem systemu ostrzegania i reagowania kryzysowego oraz ograniczania asymetrii informacyjnej (Zaskórski P., 2012).

2. ISTOTA I WYBRANE ZASTOSOWANIA INTERNETU RZECZY

Często przytaczaną w literaturze przedmiotu definicją Internetu rzeczy jest zaproponowana przez International Telecommunication Union (ITU), określająca IoT jako globalną infrastrukturę dla społeczeństwa informacyjnego, umożliwiającą dostęp do zaawansowanych usług przez połączenie (fizyczne lub wirtualne) przedmiotów (obiektów), bazujące na istniejących i rozwijanych interoperacyjnych technologiach informacyjno-komunikacyjnych (*Telecommunication Standarization…* 2006). Idea samego Internetu rzeczy pojawiła się w artykule M. Weisera „The Computer for 21st Century" (Weiser,1991, s. 94-104). Samego zaś terminu Internetu rzeczy (Internet of Things – IoT) jako pierwszy użył w swojej prezentacji K. Aszton w 1999 roku wykonanej dla koncernu Procter&Gamble (*Aszton w swej prezentacji powiązał pojęcie Internetu rzeczy z koncepcją wykorzystania Radiowych Systemów Automatycznej identyfikacji (Radio Frequency Identification RFID)w łańcuchach dostaw koncernu Procter&Gamble).* W swoich późniejszych rozważaniach Aszton zauważył, że problem rozwoju Internetu stanowią ludzkie ograniczenia co do przechwytywania informacji o świecie rzeczywistym (Aszton, 2009, nr 22, s. 97-114). Maszyny i komputery bazowały wtedy na danych wprowadzanych bezpośrednio przez ludzi. Kluczem poprawy i podstawą rozwiązania tego problemu będzie umożliwienie urządzeniom samodzielnego pozyskiwania i przetwarzania danych, aby lepiej poznawać i opisywać („danetyzować") otaczającą rzeczywistość. Dzięki temu zgodnie z koncepcją Internetu rzeczy poprzez automatyzację coraz to większej liczby procesów można w dużym stopniu ograniczać straty i niepotrzebne koszty oraz marnotrawstwo czasu.

Koncepcja Internetu rzeczy jest połączeniem w jedną sieć niemalże wszystkich (potrzebnych w danej sytuacji) rodzajów urządzeń (rzeczy), według której urządzenia te połączone za pomocą odpowiedniej infrastruktury mogą dostarczać wielu informacji z wykorzystaniem nowych usług i aplikacji. Rozwój IoT jest ściśle powiązany z nowymi usługami, które mogą być pochodnymi powstałej (zintegrowanej) infrastruktury. W swojej strukturze komunikacyjnej zawiera dwa główne rodzaje połączeń:

– między ludźmi a przedmiotami,
– przedmiotami (obiektami) między sobą.

Ten ostatni typ połączeń nazywany jest komunikacją M2M. Rozwój technologii urządzeń, które będą umożliwiały komunikację M2M lub inaczej mówiąc rzeczy między sobą będzie podstawową determinantą i wyznacznikiem dalszego rozwoju i wykorzystania Internetu rzeczy. Często w literaturze przedmiotu przedstawia się koncepcję Internetu jako zjawisko bazujące na trzech wymiarach (Brachman, 2013):

– zawsze (ANY time),
– wszędzie (ANY place),
– ze wszystkim (ANY thing).

Internet Rzeczy zapewnia więc komunikację zawsze, wszędzie i każdemu urządzeniu rezydującemu w dowolnej sieci. Aktualnie coraz częściej mówi się o rozszerzonym pojęciu Internetu rzeczy a mianowicie o Internecie wszechrzeczy. W takim ujęciu system będą tworzyć nie tylko przedmioty, ale także ludzie, zwierzęta i procesy oraz dane o wielu zjawiskach zachodzących w przyrodzie. „Wszystko" może być potraktowane jako zmienna, ale jednocześnie jako generator danych opisujących dane zjawisko lub jego stan.

„Narodziny pełnego" Internetu rzeczy można postrzegać w sposób umowny, gdzie graniczną linią jest zapewne moment przekroczenia pewnej dużej liczby podłączonych w sieć urządzeń czy rzeczy. Graniczną datą ery IoT wg Cisco Internet Business Solutions Group (Cisco IBSG) jest moment, kiedy liczba podłączonych do Internetu urządzeń i obiektów przekroczyła liczbę ludności naszego globu. Ponadto przyjmuje się, że Internet rzeczy jest pierwszą ewolucją Internetu sygnalizującą swoisty skok rozwojowy, który w niedalekiej przyszłości może doprowadzić do znacznej poprawy życia ludzi w niemal wszystkich dziedzinach życia. Już teraz można zaobserwować swoiste usprawniania w niektórych obszarach życia poprzez monitoring i analizę wielu czynników za pomocą urządzeń podłączonych do sieci. Począwszy od ochrony zdrowia i życia pojedynczego człowieka a skończywszy na monitorowaniu i analizie zagrożeń całych aglomeracji, państw i podmiotów międzynarodowych. Dalsza ewolucja Internetu w IoT doprowadzi zapewne do upowszechnienia pełnej „danetyzacji" zjawisk i procesów, czyli zbierania, gromadzenia, przetwarzania, przesyłania i rozpowszechniania danych na masową skalę, co może przynieść dużo korzystnych zjawisk (Nowakowski, Czajkowski, 4/2016), ale i kolejnych zagrożeń dla bezpieczeństwa różnych klas podmiotów a więc także generowania sytuacji kryzysowych a nawet konfliktów.

Celem Internetu rzeczy jest więc stworzenie inteligentnych obiektów i przestrzeni (inteligentnych miast – smart city, transportu, produktów, budynków, systemów energetycznych, systemów zdrowia, inteligentnych systemów bezpieczeństwa itd.). Zastosowanie IoT jest dzisiaj szerokie i dynamicznie się zwiększa dzięki jego ciągłemu rozwojowi i implementacji w większości produkowanych i tworzonych przez człowieka urządzeniach i rzeczach. (tabela 1). Jego osiągnięcia wykorzystywane są w wielu systemach bezpieczeństwa ze szczególnym akcentem kładzionym na problemy zapewniania bezpieczeństwa kryzysowego, publicznego, jak również bezpieczeństwa wybranych procesów produkcyjno-usługowych i administracyjno-zarządczych.

Tabela 1. Wybrane obszary zastosowań Internetu rzeczy

Sektory zastosowań	Wybrane obszary zastosowań	Przykłady urządzeń
1	2	3
Sektor IT	wyposażenie biur, infrastruktura biurowa, urządzenia transmisji mobilnej, sieci publiczne	samoregulacyjne klimatyzacje, inteligentne drukarki, VTC, itd.
Opieka zdrowotna	Systemy monitorujące pacjentów, telemedycyna, nowe leki, chirurgia, operacje na odległość	inteligentne protezy kończyn ,opaski monitorujące funkcje życiowe, biomedyczne chipy, itd.
Bezpieczeństwo: publiczne, wewnętrzne, zewnętrzne	monitorowanie środowiska (terenów zalewowych, oczyszczalni ścieków), informacjemeteorologiczne i klimatyczne, śledzenie ludzi, zwierząt, przesyłek czy bagażu	czujniki monitorujące infrastrukturę krytyczną, czytniki linii papilarnych, systemy rozpoznawania twarzy, inteligentne bramki na lotniskach, drony i urządzenia monitorujące smog w miastach, drony (wojskowe, cywilne)
Transport	zarządzanie flotą pojazdów, systemy informacji dla pasażerów, systemy płatności za korzystanie z infrastruktury transportowej i parkingowej	drony pocztowe, sterowanie ruchem i sygnalizacją uliczną, zielona fal, inteligentne samochody inteligentny monitoring parkingów GPS w środkach transportowych, itp.
Przemysł	produkcja monitorowanie i śledzenie produktów przemysłowych, – analiza lokalizacji dla szerokiej gamy procesów fabrycznych	automatyczne linie produkcyjne z analizą i kontrolą jakości, roboty przemysłowe
Nauka	wspomaganie doświadczeń naukowych, baza danych naukowych	inteligentne urządzenia analizy laboratoryjnej, e-biblioteki, e-booki.
Sektor detaliczny	systemy sieciowe i urządzenia, zarządzania łańcuchem dostaw, zarządzaniie informacją o produktach i konsumentach, zarządzanie zapasami	maszyny sprzedające, automatyczne stacje tankowania, maszyny do gier, e-zakupy, e-sklepy
Konsumpcja i dom	bezpieczeństwo domu – sterowanie urządzeniami, energią i oświetleniem w domu, rozrywka	smart dom, elektroniczne nianie,, aktywny monitoring i systemy samo-alarmujące, smart city, itp.

Tabela 1 cd.

1	2	3
Energetyka	wydobycie surowców poszukiwania alternatywnych, w tym odnawialnych źródeł energii, urządzenia dostarczające prąd do odbiorców	aplikacje i urządzenia do ekstrakcji surowców i ich transportu, zdalne liczniki energii elektrycznej, wykrywanie surowców naturalnych, roboty
Budownictwo	Inteligentne budynki, systemami bezpieczeństwa w budynkach itp.	systemy sterowania budynkami, osiedlami, obiektami, automatyzacja budynków
Inne	Technologie kosmiczne, sztuczna inteligencja, sieci neuronowe, itd.	systemy obróbki dużej ilości danych, systemy Big-Data

Źródło: opracowanie własne na podstawie [Beecham Research 2016; Senkus i in. 2014].

Internet rzeczy może być ważną platformą informacyjno-integracyjną dla różnych klas systemów bezpieczeństwa wewnętrznego i zewnętrznego państwa oraz lokalnych podmiotów gospodarczych. Korzystając z możliwości IoT zakłada się, że może to być wielopłaszczyznowa platforma implementacji koncepcji integracji obiektów, procesów i systemów zarządzania kryzysowego.

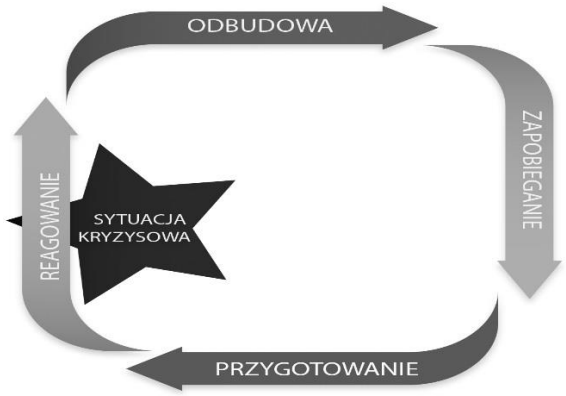
3. IDENTYFIKACJA PROCESÓW I SYSTEMU ZARZĄDZANIA KRYZYSOWEGO

Każdy podmiot narażony jest na określone ryzyko wystąpienia zakłóceń w jego funkcjonowaniu i utratę ciągłości działania, a w tym ciągłości informacyjno-decyzyjnej. Ten typ ryzyka jest zapewne groźny dla każdego podmiotu, ale w perspektywie zarządzania (kierowania) państwem postrzegamy cały kontekst różnych klas zagrożeń, które mogą skutkować sytuacją kryzysową i potrzebą ochrony jego infrastruktury krytycznej, gwarantującej niejako przetrwanie. Powstaje wtedy problem tzw. zarządzania kryzysowego w skali makro (a właściwie zarządzania w warunkach kryzysu (sytuacji kryzysowej) lub po prostu kryzys). Zjawisko to może dotyczyć – jak wcześniej wspomniano – również skali mikro (pojedynczej organizacji a nawet pojedynczego obywatela).

W obliczu coraz to nowszych wyzwań współczesności związanych z szeroko pojętą globalizacją oraz rozwojem technologii zarządzanie kryzysowe nabiera szczególnie ważnego znaczenia, stając się bardzo ważnym obszarem działania (Dz.U. z 2007, nr 89, poz. 590 z póź. zm.) i obejmuje zarządzanie organizacją (systemem) pod presją czasu a często i niedoboru zasobów. Oznacza to, że ten rodzaj zarządzania służy głównie rozwiązywaniu nietypowych sytuacji. Dostęp do odpowiedniej informacji może limitować skuteczność tych działań w zakresie zapobiegania, przeciwdziałania i reagowania w przypadku wystąpienia zakłóceń stabilno-

ści oraz przywracania stanu normalnego sprzed wystąpienia zakłócenia. Tak więc w zarządzaniu kryzysowym istotnym i najważniejszym czynnikiem przeciwdziałania sytuacjom kryzysowym jest informacja o zagrożeniu oraz sprawny i terminowy jej przepływ między strukturami i organami wchodzącymi w skład systemu zarządzania kryzysowego danego podmiotu. Jest więc de facto zarządzaniem ryzykiem utraty ciągłości działania, a w tym informacyjnej ciągłości działania organizacją w celu eliminacji i przeciwdziałania eskalacji niebezpiecznych zjawisk i trudnych sytuacji.

W całym systemie zarządzania kryzysowego zachowany jest hierarchiczny podział w obszarze całej administracji publicznej począwszy od najniższego szczebla samorządowego aż do szczebla centralnego, gdzie zadania realizowane są przez poszczególne urzędy centralne i instytucje oraz ministerstwa, aż po najwyższe osoby w państwie. W momencie wzrostu skali zagrożenia czy zwiększenia jego skutków i utraty możliwości pełnej kontroli nad zagrożeniem – zarządzanie kryzysowe jest przekazywane organom o większym potencjale. Hierarchizacja taka ma na celu zapobieganie automatycznemu uruchomieniu kosztownego, najwyższego poziomu krajowego systemu zarządzania bez próby podjęcia likwidacji zagrożenia przez organy niższego szczebla.



Rys. 1. Fazy zarządzania kryzysowego. Źródło: opracowanie własne na podstawie (Dz.U. z 2007, nr 89, poz. 590 z póź. zm.)

W zarządzaniu kryzysowym wyodrębnia się fazę zapobiegania, przygotowania oraz reagowania i odbudowy (rys. 1). Wszystkie te fazy są ze sobą informacyjnie i zadaniowo sprzężone. Szczególnego znaczenia nabierają tu fazy zapobiegania i reagowania, w których widoczna może być szczególna przydatność platformy IoT. Tworzony jest więc swoisty łańcuch bezpieczeństwa, który powinien być sprawny informacyjnie i spójny decyzyjnie w całym procesie zarządzania kryzysowego.

W fazie zapobiegania – są realizowane zadania mające na celu eliminację lub redukcję prawdopodobieństwa wystąpienia sytuacji kryzysowej (zagrożenia) oraz w razie wystąpienia ograniczające jej skutki. Podstawowym zadaniem w tej fazie jest monitorowanie, analizowanie i prognozowanie rozwoju zdarzeń/sytuacji pod kątem możliwości wystąpienia zagrożenia w danym miejscu i czasie.

W fazie przygotowania – określa się sposoby i środki niezbędne do reagowania w razie wystąpienia zagrożenia. Na tym etapie ocenia się potencjalne zagrożenia, i powinny być prowadzone działania planistyczne (opracowane szczegółowe plany i procedury działania w sytuacjach niebezpiecznych) oraz przeprowadzona prognoza sił i środków niezbędnych do podjęcia i prowadzenia działań ratowniczych.

W fazie reagowania – następuje bezzwłoczne działanie, które jest sprawdzianem efektywności i poprawności realizacji procedur i zadań zarządzania kryzysowego wykonywanych w fazie przygotowania. Na tym etapie mogą kumulować się wszystkie zaniedbania powstałe w dwóch poprzednich fazach.

W fazie odbudowy – realizuje się działania mające na celu przywrócenie zdolności reagowania, odbudowę zapasów służb ratowniczych oraz odtworzenie kluczowej dla funkcjonowania państwa infrastruktury telekomunikacyjnej, energetycznej, paliwowej, transportowej i dostarczania wody.

Wymienione fazy zarządzania kryzysowego tworzą łańcuch działań warunkowany aspektami prawnymi. Analizując wcześniej wspomniane fazy możemy przypisać do każdej z nich potrzeby, jakie są wymuszane przez przedsięwzięcia w poszczególnych etapach ich realizacji, aby cały system reagowania kryzysowego był sprawny i kompatybilny wzajemnie. Spełnienie potrzeb wymuszanych w poszczególnych fazach zarządzania kryzysowego i stopień ich spełniania jest miarą i siłą łańcucha bezpieczeństwa w systemach zarządzania kryzysowego. Każda z faz cechuje się koniecznością przetwarzania i obróbki dużej ilości danych. W przypadku systemów reagowania kryzysowego przetwarzanie informacji cechuje duża turbulentność (dynamika zmian) oraz potrzeba gromadzenia, aktualizowania i intensywnego udostępniania wyników analiz i ocen oraz wypracowanych decyzji.

Tak więc, potrzeby systemu zarządzania kryzysowego są szybkozmienne i determinowane bieżącą oceną poziomu realizacji zamierzonego celu. W zarządzaniu kryzysowym celem jest bowiem zapobieganie kryzysom lub w przypadku ich wystąpienia przejęcia nad nimi kontroli i likwidacji skutków a na koniec odbudowanie niezbędnych obiektów i zasobów infrastruktury, w tym takich składowych, które zapewnią jak najlepsze i najszybsze (determinanta czasowa) osiągnięcie wcześniej wspomnianego celu. Stąd też w zarządzaniu kryzysowym szczególnego znaczenia nabiera:

– skuteczne monitorowanie środowiska pod względem możliwości wystąpienia kataklizmów naturalnych, klęsk żywiołowych (powodzi, susz, pożarów) i innych kataklizmów naturalnych oraz możliwości wystąpienia nieprzewidzianych sytuacji społecznych,
– modernizacja infrastruktury krytycznej oraz ciągła jej kontrola i ochrona,

- monitorowanie i zbieranie danych o potencjalnych źródłach zagrożenia w środowisku naturalnym i społecznym,
- usprawnienie działań i efektywniejsze wykorzystywanie sił oraz środków koniecznych do reagowania w sytuacjach kryzysowych,
- możliwości przyspieszania akcji ratowniczych (synergia różnych systemów) i usprawnienie procedur,
- tworzenie baz i hurtowni danych na potrzeby systemów zarządzania kryzysowego,
- monitorowanie infrastruktury osiedli i całych miast pod względem bezpieczeństwa oraz monitorowanie zanieczyszczeń środowiska miejskiego i wiejskiego oraz zagrożeń epidemiologicznych (poziom smogu, jakość wody, jakość powietrza itd.),
- ciągłe doskonalenie ogólnokrajowego systemu powiadamiania państwowych służb ratunkowych (straży pożarnej, policji, pogotowia ratunkowego, straży granicznej, wojska i innych organizacji bezpieczeństwa wewnętrznego i zewnętrznego).

Potrzeby informacyjne systemu zarządzania kryzysowego i ich specyfika będą zależne od wielu czynników takich jak, poziom zagrożeń oraz ich wielkość i rozległość (globalizacja). Ponadto podstawowym wymuszeniem jest ograniczoność czasu (krótki czas reakcji na sytuację kryzysową), niepewność decyzji w warunkach braku lub nawet nadmiaru informacji (tzw. chaos informacyjny) oraz zdegenerowany (często skrócony) proces decyzyjny, co może utrudniać zaspokojenie wcześniej wspomnianych potrzeb (Sobolewski, 2011, s. 13-14). Aby system zarządzania kryzysowego państwa działał w należyty sposób i spełniał wymagania obecnych standardów międzynarodowych i krajowych niezbędna jest poprawa jakości wszystkich jego elementów. Stąd też ważnym jej czynnikiem mogą być usługi w chmurze obliczeniowej (CC) i zastosowania Internetu rzeczy (IoT).

4. ZARYS KONCEPCJI WYKORZYSTANIA INTERNETU RZECZY W SYSTEMACH ZARZĄDZANIA KRYZYSOWEGO

Turbulentny świat to świat zagrożeń i wzmożonego ryzyka. Skłania to jednak do konstatacji, że wykorzystanie IoT może redukować niektóre zjawiska, ale i może powodować dodatkowe zagrożenia, a więc wzrost turbulencji w każdym podmiocie i jego otoczeniu. Niemniej jednak zapewnianie ciągłości działania, a w szczególności ciągłości informacyjnej wydaje się być wyzwaniem dla wykorzystania idei IoT.

W systemach zarządzania kryzysowego ma zastosowanie wiele dziedzinowych rozwiązań informatycznych, w tym informatyczne systemy transakcyjne oraz analityczne klasy BI wspomagane systemami informacji geoprzestrzennej (GIS). Systemy te jednak mają w wielu przypadkach dość ograniczony poziom komplekso-

wości i integracji. Wydaje się, że koncepcja wykorzystania Internetu rzeczy (IoT) może stanowić dobrą platformę integracyjną. Połączenie urządzeń, ludzi, przedmiotów w globalną lub nawet lokalną sieć rzeczy, łączącą różne obiekty (w tym komputery, urządzenia i ludzi) z zapewnieniem wzajemnej bieżącej komunikacji – może wpłynąć na poziom bezpieczeństwa oraz jakość jego odczuwania przez ludzi, zwłaszcza w sytuacjach zagrożeń i kryzysów.

4.1. Podstawowe założenia koncepcji

Inteligentny dom – może być dobrym przykładem integracji różnej klasy urządzeń, a jego idea bazuje na połączeniu różnych urządzeń domowych i sterowanie nimi w sieci Internet. Same dostosowują się do potrzeb użytkownika wykorzystując rozległą gamę sensorów i czujników. Główną korzyścią może być bezpieczeństwo, wykraczające znacznie poza alarmy antywłamaniowe. Systemy inteligentnego domu to zbiór podsystemów wykrywania zagrożeń typu: dymu, gazu, tlenku węgla (czadu) oraz podsystemy monitorowania różnych mediów (czujniki wody, ciśnienia, zamontowane w różnych filtrach, itd.), które mogą być bezpośrednio połączone z pobliskimi posterunkami służb ratunkowych.

Bardziej kompleksowym przykładem środowiska implementacji technologii IoT może być *Smart city,* co w literaturze przedmiotu często określane jest jako idea inteligentnego miasta (Piskorz-Ryń IOT s 161). Według Michaela Millera (2016, s. 307) inteligentne miasto zaczyna się od inteligentnej infrastruktury. Często wskazuje się sześć wymiarów, które muszą zaistnieć, aby mówić o koncepcji inteligentnego miasta (Stawiasz , i in., nr 29, 2012, s. 100):

1. Gospodarka (*smart economy*).
2. Transport i komunikacja (*smart mobility*).
3. Środowiska(*smart environment*).
4. Ludzie (*smart people*).
5. Jakość życia (*smart living*).
6. Inteligentne zarządzanie (*smart governance*).

Założenia i rozwiązania inteligentnego miasta obejmują efektywniejsze wykorzystanie posiadanych zasobów publicznych, podniesienie jakości usług, obniżenie kosztów, zwiększenie bezpieczeństwa, rozwój i zmniejszenie biurokratyzmu w administracji. W praktyce będzie to oznaczało podniesienie wszystkich standardów życia społecznego i kulturalnego mieszkańców (lepsze gospodarowanie, i zarządzanie obszarami, budynkami, utylizacja odpadów, obniżenie kosztów energii elektrycznej i zużycia mediów). Inteligentne miasto bazuje więc na IoT i danych zbieranych i przetwarzanych przez inteligentne urządzenia w całym jego otoczeniu.

Przyjmując, że koncepcja smart city, jest dobrym obrazem implementacji Internetu rzeczy w niemalże wszystkich dziedzinach życia miasta, to dostrzegamy pewien model bazowy rozwoju IoT. Na podstawie analizy dostępnych rozwiązań

mogą być sformułowane wymagania dla obszaru bezpieczeństwa a ściślej dla systemów zarządzania kryzysowego. Wdrożenie idei IoT w celu wzbogacenia funkcjonalności systemów zarządzania kryzysowego otwiera nowe możliwości zapewniania ciągłości działania i ograniczania ryzyka ekologicznego, energetycznego, przyrodniczego, zdrowotnego, komunikacyjnego, socjalnego i innych. Analizując możliwość wystąpienia różnorakich zagrożeń i kataklizmów oraz potrzebę natychmiastowego przeciwdziałania im – wykorzystanie Internetu rzeczy wydaje się naturalnym sposobem doskonalenia systemów reagowania kryzysowego. Internet rzeczy – w dużej mierze sieci M2M (Machine-To_Machine), gdzie główną rolę pełni komunikacja między urządzeniami i generowane przez nich dane gromadzone są w systemach bazodanowych (a dziś coraz częściej odwołujemy się do systemów analitycznych typu OLAP lub więcej, czyli Big Data). Zgromadzona wiedza umożliwia samodzielność i skuteczność procesów decyzyjnych poprzez (Sakowska-Baryła, s. 137):

– umożliwienie identyfikacji każdego komponentu danego systemu (w tym tzw. autodane),
– zapewnienie komunikacji (wszystko może się komunikować ze sobą),
– współdziałanie (wszystko może na siebie oddziaływać).

Podstawą implementacji IoT w systemie zarządzania kryzysowego mogą być – założenia modelu architektury ICT, a dokładniej architektury technologii informacyjno-komunikacyjnych (Information Communication Technology – ICT).

ICT zwana też architekturą przedsiębiorstwa lub korporacji obejmuje zasady graficznej prezentacji struktur technologicznych i systemów informatycznych. Jest odzwierciedleniem całości metod, zasad i modeli wykorzystywanych w projektowaniu i realizacji struktury organizacyjnej systemów informacji i infrastruktury dla procesów biznesowych w organizacyjnych produkcyjno-usługowych (Lankhorst, s. 3.). Według D. Minoli (s. 34) przykładem przedsiębiorstwa w odniesieniu do ICT jest cała korporacja, jej wydział, agencja rządowa , grupa instytucji rządowych lub cały system ratownictwa. Kompleksowa architektura przedsiębiorstwa tworzona jest za pomocą odpowiedniej metodyki, która operuje modelami, technikami, językami specyfikacji i opisów oraz narzędziami analizy dziedziny przedmiotu projektowania (pojęciowego, logicznego, fizycznego). W analizie przedsiębiorstwa powinna być stosowana zasada dekompozycji pewnej całości oraz zasada abstrakcji, czyli świadomego pomijania mniej istotnych wątków danego przedmiotu analizy oraz wyodrębnienie cech wspólnych i zbioru niezmienników (Bazewicz, s. 30).

Podstawowym celem rozwoju systemów zarządzania kryzysowego powinno być ujęcie systemowe i integracja potrzebnych/istotnych obiektów na platformie IoT w organizacjach typu korporacja, gmina, województwo, powiat i całe państwo przez analogię do modelu ICT powiązanego ze strategią organizacji biznesowej. Architektura organizacji biznesowej powinna sprzyjać lepszym możliwościom adaptacji do przemian zachodzących w świecie technologicznym i gospodarczym oraz dostosowania narzędzi do innowacyjnego zarządzania. Jeśli zastosujemy takie podejście do systemów zarządzania kryzysowego i przyjmiemy jako przedsiębior-

stwo organ administracji państwowej, jaki chcemy wspomagać to model architektury ICT będzie dobrym odwzorowaniem potrzeb w kontekście zarządzania kryzysowego. Zakłada się więc, że nasycenie systemami ICT infrastruktury krytycznej i wyposażenie jej elementarnych komponentów w różnego typu sensory oraz ich integracja powinny podwyższyć poziom bezpieczeństwa oraz zmniejszyć ryzyko wystąpienia zagrożeń. Szczególną rolę należy w systemach reagowania kryzysowego przypisać urządzeniom i rzeczom mobilnym, które są wzajemnie połączone i mają dostęp do usług internetowych oraz zapewniają interakcje między sobą oraz między użytkownikami.

4.2. Wymagania uzupełniające

Wdrożenie i wykorzystanie złożonych systemów teleinformatycznych *wiąże się z koncepcją umożliwiającą wykorzystanie istniejącej platformy teleinformatycznej, wiedzy i doświadczenia ludzi zajmujących się zarządzaniem kryzysowym.* Koncepcja ta bazuje na tzw. środowisku sieciocentrycznym (ang. Network Centric Warfare – NCW), której zadaniem jest usprawnianie procesu pozyskiwania, przetwarzania i selekcji danych z wielu źródeł oraz zagwarantowania efektywnej dystrybucji informacji, określenia zadań, ról i miejsca w złożonym systemie zarządzania kryzysowego w środowisku IoT (Żwirek, 2015).

Zastosowanie Internetu rzeczy w systemach zarządzania kryzysowego może być pewną szansą dla rozwoju całego sytemu bezpieczeństwa kraju i podniesienia jego poziomu odczuwalności. Dzięki połączeniu wszystkich urządzeń w jedną sieć, system reagowania kryzysowego może otrzymywać nowoczesne i najbardziej zaawansowane narzędzie do analizowania, komunikowania, gromadzenia, zbierania, badania i przewidywania zagrożeń oraz czynników mogących wywołać kryzys. Wyzwaniem dla gospodarki i systemów bezpieczeństwa w tym SZK naszego kraju, jak i innych państw UE jest ciągły postęp w zakresie innowacyjności. W ramach strategii „Europa 2020" UE wyznaczyła kierunki polityki na rzecz badań naukowych i innowacyjności. Wymaganiami, jakie stawiane są przed IoT jako determinantą implementacji rozwiązań w systemach ZK mogą być przede wszystkim(Benduch, s. 67):

1. Niezawodności całego systemu IoT (niska awaryjność w każdych warunkach).
2. Mobilność elementów IoT (wielopłaszczyznowe wykorzystanie IoT).
3. Względnie niska cena (koszt musi być adekwatny do rangi i poziomu całego systemu).
4. Bezpieczeństwo danych (w tym zapewnienie ochrony danych osobowych oraz odporność rozwiązań np. na ataki hakerów oraz inne mogące wystąpić zakłócenia).
5. Kompatybilność wszystkich systemów i urządzeń (interfejsy komunikacyjne) oraz ciągłość procesów zarządzania nimi.

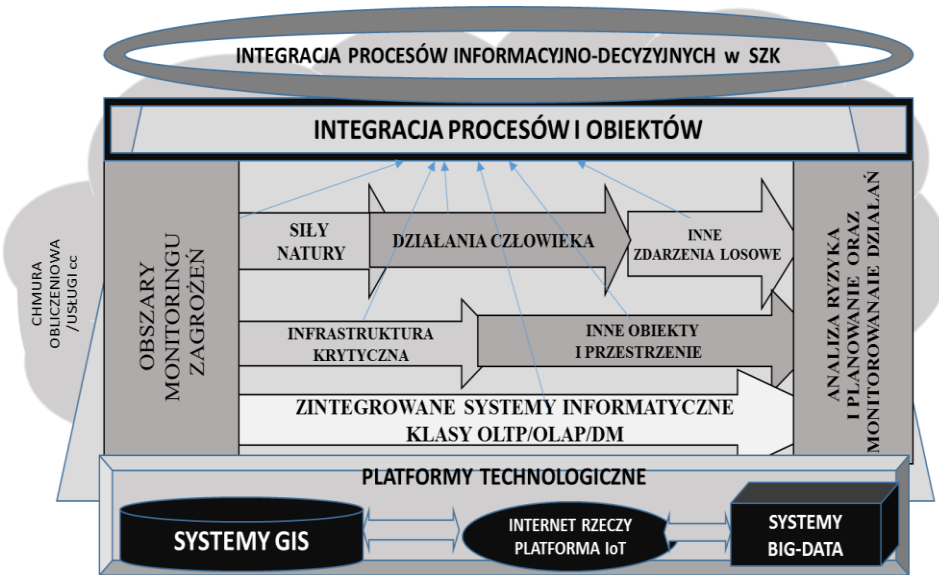
6. Konieczność sprostania wymaganiom SZK, a w tym łatwość i czas implementacji rozwiązań IoT w tych systemach.

Przedstawione wyżej wymagania opisują ramowo modelowe potrzeby wykorzystania IoT w przedmiotowych systemach i procesach zarządzania kryzysowego (SZK).

4.3. Ogólny model Systemu Zarządzania Kryzysowego z wykorzystaniem IoT

Internet rzeczy zapewnia dużo szybszą i skuteczniejszą wymianę danych i komunikację między rzeczami go tworzącymi. Stąd wg modelu docelowego (rys. 2) powstanie sieć inteligentnych obiektów gospodarczych, technicznych i administracyjnych (w tym podmioty administracji publicznej), w których systemy komputerowe oraz zintegrowane systemy informatyczne zarządzania (ZSIZ typu OLTP, OLAP z mechanizmami odkrywania wiedzy tzw. Data-Mining i inne) będą zbierać i przetwarzać duże ilości danych oraz sterować przepływem informacji (a w tym liniami produkcyjnymi, ruchem ulicznym, czy budynkami, a także różnorodnymi systemami monitorującymi cały ekosystem) o zdarzeniach bieżących z ich selekcją wg zagrożeń zarówno wynikających z działania sił natury, jak i z działalności człowieka oraz z innych zdarzeń losowych. Dostęp w trybie on-line do informacji o stanie poszczególnych obiektów objętych zagrożeniem stanie się główną wartością systemów zarządzania a szczególnie reagowania kryzysowego. Gromadzone informacje oraz dostęp do danych rezydujących w publicznych zasobach określanych mianem Big-Data mogą stanowić bazę do wieloaspektowych analiz, poszukiwania analogii i wnioskowania. Ponadto przewiduje się, że w najbliższych latach wykorzystanie IoT będzie szczególnie dynamiczne w logistyce, przemyśle, sektorze publicznym i usługach finansowych oraz w systemach bezpieczeństwa (monitorowanie infrastruktury krytycznej państwa). Stwarza to możliwości jego szerokiej implementacji w systemach zarządzania kryzysowego w wymiarze lokalnym i globalnym (integracja informacji o zasobach i zagrożeniach w kraju, regionach i organizacjach międzynarodowych) ze szczególnym uwzględnieniem monitoringu zjawisk naturalnych i społeczno-gospodarczych. Bardzo ważną platformą technologiczną w analizach geoprzestrzennych ryzyka wystąpienia zagrożeń jest platforma systemów GIS (może być dostępna także jako usługa w chmurze obliczeniowej), która w połączeniu z wymiarem geograficznym dyslokacji sił i środków w systemach reagowania kryzysowego może stanowić nieoceniony materiał analityczny, wspomagający procesy planowania i nadzorowania (monitorowania) sytuacji kryzysowej i podejmowanych adekwatnych działań. Dzięki dostępowi do aktualnych danych (systemy OLTP) o sytuacji w różnych wymiarach analitycznych (systemy OLAP, systemy Big_Data) i ze zobrazowaniem bieżącej sytuacji na mapach cyfrowych możliwa jest nie tylko integracja procesów roboczych i związa-

nych z nimi obiektów, ale przede wszystkim integracja procesów informacyjno-decyzyjnych ze szczególnym uwzględnieniem ich integralności, kompletności i spójności przestrzenno-czasowej.



Rys. 2. Ramowy model wykorzystania IoT w integracji SZK (opracowanie własne)

Istnieje wiele analogii dla wykorzystania zarówno możliwości IoT, jak również zastosowań usług CC (Cloud Computing). Szwecja od 2013 roku wykorzystuje sieć połączonych sensorów zanurzonych w rurach do odprowadzania ścieków w celu wykrywania chemikaliów służących do budowy materiałów wybuchowych tzw. domowej produkcji (Projekt EMPHASIS finansowany ze środków Unii Europejskiej, a realizowany pod nadzorem Szwedzkiej Agencji Rozwoju Obronności/ (FOI), Fiddian. 2013). Nicea zaimplementowała cztery inteligentne usługi w mieście bazujące na Internecie rzeczy: inteligentne zarządzanie ruchem samochodowym (i miejscami parkingowymi), inteligentne oświetlenie, inteligentny system wywozu śmieci oraz monitorowanie parametrów środowiska. Całość bazuje na czterowarstwowym modelu (warstwa aplikacji, warstwa usług, warstwa sieci oraz warstwa sensorów, Mitchell i in. 2013). Wprowadzenie tego rodzaju rozwiązań z pewnością poprawia jakość i gwarantuje polepszenie bezpieczeństwa lub ogranicza ryzyko realizacji wybranych zagrożeń. W Amsterdamie od 2012 współpracując z firmami Cisco oraz Philips zainstalowano inteligentny system oświetlenia ulicznego wykorzystujący lampy LED. Każda z lamp została wyposażona w sensory i jest w stanie automatycznie zaraportować problemy związane z prawidłowym działaniem, automatycznie planuje okresowe przeglądy w taki sposób, aby jak

najmniej zakłócać ruch na ulicy i chodnikach. System umożliwia także automatycznie ściemnianie, gdy nie ma dużego natężenia ruchu oraz inteligentne planowanie (Mitchell i in. 2013).

W Polsce trwają badania i prace nad opracowaniem systemu „Wsparcia Analiz Zagrożeń Skażeniami i Alarmowania" (obecnie powstał prototyp systemu). System realizowany jest w ramach projektu NCBiR nr DOBBIO7/12/01/2015 pt. „Integracja i wsparcie procesów zarządzania informacją i optymalizacji decyzji systemu ostrzegania i alarmowania" na potrzeby Krajowego Systemu Wykrywania Skażeń i Alarmowani (KSWSiA).

Takie rozwiązania z pewnością w większym stopniu chronią i zabezpieczają systemy energetyczne jako ważne komponenty infrastruktury krytycznej państwa, ważne obiekty przemysłowe i inne elementy tej infrastruktury. Bieżące monitorowanie zagrożeń ze strony sił natury, jak i działalności człowieka jest ważnym wyzwaniem w systemach reagowania kryzysowego. Poszerzając takie rozwiązanie na coraz większą liczbę obiektów z wykorzystaniem atrybutu mobilności zyskujemy system kompleksowej i wiarygodnej informacji o zagrożeniach oraz siłach i środkach przeciwdziałania temu.

4.4. Ograniczenia koncepcji wykorzystania IoT

Podstawowymi przeszkodami i ograniczeniem w wykorzystaniu Internetu rzeczy w SZK mogą być (*http//www.forbes.pl/ znaczenie IoT w biznesie, 2017.12.04)*:

1. Duży koszt wdrażania nowych technologii i brak dostatecznej wiedzy o Internecie rzeczy (czym jest i jak może wpłynąć na rozwój oraz poprawę SZK).
2. Brak kompleksowej wizji znaczenia i wykorzystania IoT dla SZK, a w tym tempa rozwoju IoT i świadomości nowych zagrożeń.
3. Brak uregulowań prawnych co do rozwoju i wdrażania technologii IoT w SZK.
4. Niedoskonałość systemów pod względem bezpieczeństwa cyberprzestrzeni (narażenie na ataki hakerów np. haker znany jako „pr0f" włamał się do systemu zarządzania wodą i kanalizacją/SCADA w mieście Springfield/Illinois, USA. Zidentyfikowano przy tym problem słabych haseł, Townsend 2013).

Należy tu zaznaczyć, że duże znaczenie dla SZK ma dalszy rozwój „inteligentnych" przedmiotów i systemów, które sprzyjają mobilności rozwiązań IoT we wszystkich obszarach bezpieczeństwa państwa. Prowadzone są prace nad systemami monitorowania obiektów o szczególnym znaczeniu dla bezpieczeństwa państwa i ludności, a w tym nad systemami monitorowania i ostrzegania obiektów publicznych (lotnisk, dworców i innych) oraz urządzeń powszechnego użytku (windy, środki komunikacji publicznej, bankomaty itp.). Uzyskane wyniki badań empirycznych i podejmowanych projektów badawczo-rozwojowych będą publikowane przez autorów w kolejnych raportach.

5. PODSUMOWANIE

Platforma Internetu rzeczy może sprzyjać nie tylko spójności i informacyjnej integralności procesów decyzyjnych, ale także determinować efektywność procesów decyzyjnych w systemach zarządzania kryzysowego i procesów logistycznych w systemach reagowania kryzysowego. Są to dwa obszary silnie wpływające na ciągłość działania w sytuacjach zagrożeń i kryzysów. Platforma IoT niesie jednak nie tylko nowe możliwości, ale może generować nowe zagrożenia, które mogą stanowić dodatkowy problem we wdrażaniu różnego rodzaju systemów bazujących na urządzeniach IoT. Jednakże odpowiednie ich przygotowanie i wprowadzenie zabezpieczeń pozwoli na zwiększenie elastyczności, spójności i efektywności podejmowanych działań. Zaprezentowany tu zarys koncepcji jest pewną przesłanką do dalszych badań i projektów badawczych, które będą podejmowane.

Współczesne SZK stanowią kompleks narzędziowo-informacyjny z uwzględnieniem możliwości bieżącego informowania w trybie on-line o potrzebach i możliwościach działania. Złożoność tej klasy systemów działania i ich dynamika zmian w otoczeniu oraz we współdziałaniu z różnymi podmiotami potwierdzają przydatność bazy techniczno-technologicznej platformy IoT. Koncepcja zastosowania Internetu rzeczy w systemach zarządzania kryzysowego jest rozwiązaniem perspektywicznym. Ciągły rozwój IoT daje duże możliwości w poprawie jakości życia i w zapewnianiu bezpieczeństwa państwa i jednostki. Sprawnie funkcjonujące systemy zarządzania kryzysowego pozwalają zawczasu wykryć objawy, minimalizować ryzyko z nimi związane oraz w razie wystąpienia sytuacji kryzysowej - skuteczniej je ograniczać, a nawet likwidować. Aby zapewnić sprawność i niezawodność systemów reagowania kryzysowego musimy zadbać o jego ciągłe doskonalenie. Rozwiązaniem, które może zapewnić sprawniejsze funkcjonowanie SZK jest platforma Internetu rzeczy, która daje nieograniczone praktycznie możliwości implementacji i stwarza warunki ciągłego rozwoju oraz innowacyjności w tej dziedzinie.

LITERATURA

Aszton, K. (2009). That "Internet of Things" Thing. *RFiD Journal,* 22, 97-114.

Brachman, A. (2013). *Internet przedmiotów. Raport Obserwatorium ICT*. Gliwice: Park Naukowo-Technologiczny „Technopark Gliwice". Retrieved from http://www.technopark.gliwice.pl/files/artykuly/Internet%20 przedmiot%C3%B3w.pdf (1.12.2017).

Cripe, F. (2013). Internet of Things: Evolving transactions into relationships. *Technology forecast,* 1.

Evans (2011). *The Internet of Things – How the Next Evolution of the Internet is Changing Everything*. CISCO IBSG White Paper, 04., 2.

Fiddian, P. (2013). *Explosives Sensors Detect Sewer Chemicals*, Copybook, 6.11.2013, http://www.copybook.com/security/news/explosives-sensorsdetect-sewer-chemicals (15.01.2017).

International Telecommunication Union (2012). *Next Generation Networks – Framework and functional architecture models – Overview of the Internet of things*, ITU-T Y.2060, 06/2012, 2-3.

Kmiecik, P. (2015). *Wykorzystanie teleinformatycznych systemów zarządzania informacją w zarządzaniu kryzysowym.* Pobrane z: *http://www.nowastrategia.org.pl/itwzk/* (17.02.2018).

Lankhorst, M. (2017). *Enterprise Architecture at Work*. Springer.

Miller, M. (2016). *Internet rzeczy, jak inteligentne telewizory, samochody, domy i miasta zmieniają świat.* Warszawa: PWN.

Minoli, D. (2008). *Enterprise Architecture A to Z*., CRC Press, 34.

Mitchell, S., Villa, N., Stewart-Weeks, M., Lange, A. (2013). *The Internet of Everything for Cities.* San Jose: Cisco Press.

Nowakowski, W., Czajkowski, R. (2016). IoT jako naturalna ewolucja Internetu. Technika Informacyjna. *Elektronika*, 4.

Piskorz-Ryń, A. (2015). *Internet of Things. Ponowne wykorzystanie zasobów w smart city.* Warszawa: C.H. Beck.

Sobolewski, G. (2011). *Organizacja i funkcjonowanie centrum zarządzania kryzysowego.* Warszawa: AON.

Szoper, G., (red.) (2015). *Internet rzeczy. Bezpieczeństwo w smart city.* Warszawa: Wyd. C.H. Beck.

Stawiasz, D. et al. (2012). Koncepcja Smart City jako wyznacznik podejmowania decyzji związanych z funkcjonowaniem i rozwojem miast. *Zeszyty naukowe USZ Studia Informatica*, 29.

Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. z 2007 Nr 89, poz. 590 z póź. zmianami).

Weiser. M. (1991). The Computer for the 21 st century. *Scientific American*, 265(3), 94-104.

Vermesan, O., Friess, P. (eds.) (2014). *Internet of Things Strategic Research and Innovation.* Agenda, 11.

Zaskórski, P. (2012). *Asymetria informacyjna w zarządzaniu procesami.* Warszawa: Wydawnictwo WAT.

Zaskórski, P. (2011). *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*. Warszawa: Wydawnictwo WAT.

Sienkiewicz, P., Świeboda, H., Wieleba, R., Żwirek, K. (2018). *Model regionalnego inteligentnego systemu wspomagania decyzji o użyciu zasobów logistycznych ratownictwa*. Retrieved from: http://csikgw.wp.mil.pl/pl/30_8.html (12.02.2018).

Ministerstwo Cyfryzacji (2018). Retrieved from: *https://obywatel.gov.pl/dokumenty-i-dane-osobowe/mdokumenty* (12.02.2018).

IMPLEMENTATION OF THE INTERNET OF THINGS (IoT) IN THE INTEGRATION OF CRISIS MANAGEMENT PROCESSES

Summary

The article presents an outline concept of using the Internet of Things (IoT) in crisis management processes. Also presented are the resulting benefits and the related risks. An attempt is made to identify the extent and the domains of the use of the Internet of Things in broadly defined security systems. This discussion encourages a broader approach to the Internet of Things and underscores its role and importance in the fast changing world which is exposed to ever new dangers accompanying technological development and globalization. These dangers require the strengthening and perfecting of crisis management systems, particularly for the purpose to assure the informational continuity of functioning.

Keywords: internet of things, (IoT), crisis management, smart city