Neural Computing and Applications
https://doi.org/10.1007/s00521-021-06720-1

S.I.: IOT-BASED HEALTH MONITORING SYSTEM

A cyber warfare perspective on risks related to health IoT devices and contact tracing

Andrea Bobbio[1] · Lelio Campanile[2] · Marco Gribaudo[3] · Mauro Iacono[2] · Fiammetta Marulli[2] · Michele Mastroianni[2]

Received: 3 January 2021 / Accepted: 30 October 2021

Abstract

The wide use of IT resources to assess and manage the recent COVID-19 pandemic allows to increase the effectiveness of the countermeasures and the pervasiveness of monitoring and prevention. Unfortunately, the literature reports that IoT devices, a widely adopted technology for these applications, are characterized by security vulnerabilities that are difficult to manage at the state level. Comparable problems exist for related technologies that leverage smartphones, such as contact tracing applications, and non-medical health monitoring devices. In analogous situations, these vulnerabilities may be exploited in the cyber domain to overload the crisis management systems with false alarms and to interfere with the interests of target countries, with consequences on their economy and their political equilibria. In this paper we analyze the potential threat to an example subsystem to show how these influences may impact it and evaluate a possible consequence.

Keywords Cyber warfare · Risk analysis · COVID-19 · IoT · Security

1 Introduction

The COVID-19 pandemics unveiled the vulnerability of whole countries especially on their economy and social and healthcare systems. Notwithstanding the availability of advanced technologies and the penetration and pervasiveness of digitization, in many countries the need for precautions and the spread of the disease caused damages to economic activities, impacting the Gross Domestic Product (GDP) and straining the capacity of hospitals and health facilities. The press reported the significant impact of the COVID-19 pandemic and that different countries established different strategies to cope with it, such as higher or lower application of lockdowns, restrictions on commerce or economic activities, and diverse prescriptions about infected people with different symptoms, people that came to contact with infected people, people specially exposed to risks because of preexisting conditions, type of professional activity, age or other factors. This obviously had consequences on political equilibria, with regard to internal and external affairs, on public opinion and on electoral campaigns and processes. For example, EU is discussing special measures and support that are causing intense reactions in each country and between countries. Experts

✉ Michele Mastroianni
michele.mastroianni@unicampania.it

Andrea Bobbio
andrea.bobbio@uniupo.it

Lelio Campanile
lelio.campanile@unicampania.it

Marco Gribaudo
marco.gribaudo@polimi.it

Mauro Iacono
mauro.iacono@unicampania.it

Fiammetta Marulli
fiammetta.marulli@unicampania.it

[1] DiSit, Università del Piemonte Orientale, viale Teresa Michel 11, 15121 Alessandria, Italy

[2] Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", viale Lincoln 5, 81100 Caserta, Italy

[3] Dipartimento di Elettronica, Informatica e Bioingegneria, Politecnico di Milano, via Ponzio 34/5, 20133 Milano, Italy

Published online: 20 January 2022

expect major consequences on the economy of each country. Many countries are considered in need of additional funds, while the perspective of a surrender of sovereignty in exchange might be argued to be an unacceptable constraint for the future.

Technology has been widely deployed to contrast and contain the effects of the disease. Besides the great support of modern networks to distance working, when and where possible, and to partially compensate suspension of school and university attendance in some countries, two main contributions have been provided to control and manage the infection: Internet of Things (IoT), for both personal health monitoring with medical or non-medical devices, and contact tracing applications [1, 12].

The spread of IoT devices and smartphones is ubiquitous, and spans over private and public places, home and enterprise environments, with pervasiveness and mobility characteristics that make them well embedded into daily activities.

The spread of adoption and installation of these technologies causes many of these devices to be unmanaged or sloppily cared by owners or users. Even when used in an enterprise environment, it is not infrequent that such devices do not get sufficient attention or coverage, and are not integrated into normal network and computer security procedures [2]. Smartphones users are generally not power users, and tend to install unsafe applications and access unsafe contents on the Internet due to a lack of sufficient awareness of security issues. They are exposed to all general threats that are very common against commercial, general purpose devices. Design efforts for IoT devices often target features embedding and cost issues, so that it is not unlikely that off-the-shelf devices do not have enough resources or do not implement support for security-oriented features. This makes them vulnerable attack surfaces, and security concerns are raised in the literature that document known issues and cases [22]. The versatility of modern smartphones and the abundance of computing resources, storage and energy availability reached by the most recent mid-range products, together with their mobility between different mobile and public, private or home WiFi networks and the use of them as hubs for personal area sensor networks make them a very interesting vector to threaten a vast number of targets [24].

In general, this situation does produce a large number of dispersed targets, resulting in a plurality of disjoint attack surfaces that might be of interest to any type of attacker. This type of problem is in the domain of cybersecurity. If we focus of the subset of the devices that are used to cope with COVID-19 issues (and that is reasonable to expect that they will be used in future events with analogous characterization) we are shaping a well defined attack surface that may be out of reach, for the plurality of involved vendors and applications, for cybercriminals, but would be a perfect target for cyber warfare operations as well, if part of a proper strategy aiming to damage a country. In fact, the capability of provoking false, but plausible, readings on health monitoring devices or contact tracing software may be used, with appropriate strategies, to exert pressure over health facilities by producing false warnings and signal false contacts with infected people, or to provoke unnecessary mandatory self-quarantine[1] of workers. This will have adverse consequences on business, production, sustainability of commerce, freight and public transport and other sectors, including healthcare. Recent statistics show that this may actually cause loss of competitiveness, a decrease in the GDP, as well as give rise to mass protests that actually contribute to an increase in the probability of a propagation of the contagion due to crowding. It is not unlikely that cyber exploits of this kind that aim at influencing the economy, politics and international relations may be used to weaken companies in the target country and buy them to expand own economy abroad and penetrate new export markets, or to force foreign governments to accept international agreements because of a domestic instability situation, media pressure or social situation.

From a cyber warfare perspective, the large number of target devices is a minor problem, due to the scale of the effort that a state and its military cyber forces can apply. The cyber warfare domain is characterized by a large asymmetry between the attack and defense capabilities of a country, due to the ease of developing and using of cyber weapons and the difficulty of tracking attacks to their source. A comparison is possible with nuclear warfare, and an important difference is immediately evident: in fact, in cyber warfare there is, at the moment, no known way to enact confidence-building measures[2]. This is due to the lack of exhibiting weapons and allowing an estimation of own arsenal by adversaries, as well as to delimit targets and responsibilities: this makes the definition of deterrence mechanisms hard, so suggesting attack-first strategies [26]. A cyber defense setup is very hard to organize and establish, and has in prevention and proactive risk analysis the most effective weapons.

In this perspective, the attack surface of interest is composed of: (I) Bluetooth[3] or WiFi[4] contact tracing apps for smartphones; (ii) health monitoring sensors, such as sport oriented devices, smartwatches, smart bands, other

[1] This is, for example, what regulations impose in Italy.

[2] As this is a very complex topic, involving several issues, including geopolitical and strategical doctrines, we will not deal with it in detail.

[3] Such as implemented in Italy, for example.

[4] Such as implemented in London Tube, for example.

IoT devices that autonomously connect to the Internet or use smartphone apps as hubs; (iii) medical sensors that operate on the same basis; (iv) autonomous IoT devices for medical use to be used in healthcare facilities; (v) autonomous IoT devices for medical use to be used to monitor infected people at home; and (vi) independent IoT devices for other non-health related purposes, such as access monitoring. We do not include computer-hosted targets because they are more likely to be well protected and because they can be impacted by poisonous data coming from the six listed categories, that is, by their sources. While obtaining a complete catalogue of these devices is probably not viable for isolated attackers or cyberterrorists, it is not a hard task for cyber forces to build it and to explore them offline searching for possible attack strategies to enact on actual installations. While directly locating the targets on the Internet is complex, servers are more likely to be located and identified by observing operational traffic and service traffic (e.g., connections towards known update servers of the vendors).

In this paper we focus on a preliminary analysis of the risk and the global impact of similar threats in terms of cyber warfare initiatives. We target the consequence of attacks on the overall response capabilities of health-related infrastructures. The applicability of our approach is shown over the consequences of the vulnerability of smartphones as single points of vulnerability for devices of type (I), (ii) and (iii) on one of the consequence, namely, the increase in pressure on testing facilities due to false alarms resulting by the attacks.

This paper is organized as follows: after this introduction, Sect. 2 presents related work, Sect. 3 presents an analysis of the general context and of the possible effects that may motivate the attacks in the cyber warfare perspective, Sect. 4 presents the modeling approach for the analyzed target subsystem, Sect. 5 presents the model. Conclusions and future work follow.

2 Related work

The unprecedented worldwide COVID-19 pandemic has shown that currently, novel diseases severely impact public health, human society, and global economy, when health systems are unable to respond promptly and pharmaceutical treatments and vaccines are unavailable or not sufficient to combat and contain phenomena of such a large and severe scale.

One of the lessons learned from the management policies acted by the world organizations to contain the spread of the COVID-19 pandemic is that, when healthcare facilities are inadequate or temporarily run out of resources, long-term systems for preventing and controlling new infectious diseases can help to limit the damage of a pandemic.

IoT technologies, due to its ubiquitous sensing ability and seamless connectivity, have already changed our lives by introducing a smart way of thinking and acting. Examples are the smart healthcare, the smart home, and smart cities, that aim to build a more convenient and intelligent community.

The powerful capability of ubiquitous IoT devices in sensing spontaneously human features, such as activities, health conditions and vital signs, can be exploited in the emergencies management, as in the case of the COVID-19 pandemic [15], where the IoT could be incorporated into the epidemic prevention and control system.

[6] provides the review of an intelligent IoT-based platform designed for COVID-19 prevention and control that could be used in both the COVID-19 pandemic and post-pandemic periods. Specifically, the reviewed IoT platform involves five non-pharmaceutical interventions (NPIs) [8, 16] including COVID-19 Symptom Diagnosis, Quarantine Monitoring, and Contact Tracing [1] & Social Distancing, implemented in a fog layer, and the COVID-19 Outbreak Forecasting and SARS-CoV-2 Mutation Tracking, implemented in a cloud layer. In this work, authors provide a comprehensive investigation and review of the state-of-the-art studies of IoT-based monitoring and sensing, which can be used to implement these five NPIs for COVID-19 prevention and control. Finally, a map showing how to associate existing IoT platform and IoT applications with COVID-19 prevention and control is provided.

These five NPIs provide a set of basic tracks on which to base the investigation of current and future IoT based systems capabilities in countering against the current COVID-19 pandemic or future infectious disease epidemics.

So, the synergistic use of IoT infrastructures with other popular technologies, e.g., artificial intelligence (AI), fog computing or big data oriented solutions, makes feasible the extension of the COVID-19 NPIs into people's daily lives to achieve intelligent and effective prevention and control.

Moreover, the enormous amount of data provided by IoT networks can be further analyzed to perform event prediction using big data analytics and machine/deep learning techniques [25].

In the more specific context of the COVID-19 pandemic, IoT technologies have been employed massively to implement contact tracing applications [1].

COVID-19 is known to be a highly infectious virus, but infected persons may not initially exhibit symptoms, while some remain asymptomatic. Thus, a non-negligible fraction of the population can, at any given time, be a hidden source of transmission.

Contact tracing is normally accomplished by health authorities through a manual interview of the infected persons. Such interviews aim at collecting and possibly identifying the persons that came into contact with an infected person in the very near past (14–21 days incubation period for COVID-19). Such contact information can be used to estimate a risk-score of contagion for each of these contacts, based on the type of contact made (e.g., indoor or outdoor environment), its duration, and proximity (distance occurred among the contacts). However, such interviews require a considerable workforce of health officials trained in the art of manual contact tracing; on the other hand, it is quite difficult to remember every person you have come into contact with in the last three weeks. Besides, an infected person might have infected many persons that cannot be identified, such as contacts with unknown persons standing in a crowded place.

Consequently, recent research efforts have been focusing on technological solutions to automate the contact tracing process with the aim of quickly and reliably identifying contacts that might be at significant infection risk. Smartphones, due to their ubiquity and the ability to keep track of their location (e.g., via GPS and WiFi), along with their in-built Bluetooth interface allowing communication and proximity detection with other nearby smartphones, represent the ideal devices for implementing automated and reliable contact tracing. As a result, many smartphone contact tracing apps have been proposed, with some already deployed, as discussed in [1], where a comprehensive review of the most recent tracing apps is proposed along with a discussion about some critical attributes of this kind of apps, according the concerns users have reported regarding their usage.

In response to this opportunity, many governments (among which the Italian one that distributed the "Immuni" app[5]) have shown great interest in smartphone contact tracing apps that help automate the difficult task of tracing all recent contacts of newly identified infected persons. However, tracing apps have generated much discussion around their key attributes, including system architecture, data management, privacy[6], security, proximity estimation, and attack vulnerability [23].

Anyway, contact tracing applications have exposed the side to privacy related implications, as it is discussed in [5], where some ways of ameliorating the privacy concerns without decreasing usefulness to public health are discussed.

Moreover, beyond the unquestionable advantages brought by the use of IoT in monitoring and support systems for healthcare, the reliability of such systems is an essential requirement and unintentional faults or artificially caused anomalies related to these systems should not be overlooked.

Anomaly is that portion(s) of data that do not conform to the rest of the data or does not follow the expected trend or characteristics. Anomaly detection is of utmost importance in healthcare analytics, because of the significant information and interests are embedded in anomalous events.

Thus, the anomalous events are to be accurately detected with low false negative alarms often under high noise (low SNR) condition. According to the study proposed in [27], in which anomalies are discussed affecting IoT based systems for Healthcare Analytics, the main challenge of anomaly detection in medical applications is to reduce the False Negatives Rate *(FNR)*, i.e., disease should not get undetected.

A False Negative *(FN)*, like an undetected disease, may result in severe consequences, up to and including the death of persons.

Moreover, in the case of contagious and asymptomatic diseases, as it is often the case with COVID-19, a false negative in detecting the presence of the virus even in a single person results in a spreading event, since asymptomatic subjects have frequently bypassed explicit checks or, supported by false negative swab outcomes, felt free to keep on living their normal lives without taking precautions necessary to prevent the spread and transmission of the virus.

The IoT, jointly with all other emerging smart technologies, may be essential to mitigate such kind of critical situations and sometimes irresponsible behaviors held by persons, as long as they are reliable in detecting with as little uncertainty as possible potential threats.

So, it is compelling to ensure that the number of FN tends to 0. However, tuning an algorithm to minimize FN would inevitably raise the False Positives Rate *(FPR)*. But more False Positives *(FP)* would result in 'alarm fatigue', i.e., medical caregivers would ignore most of the alarms considering them FP. Such incidents would possibly be fatal.

Furthermore, beyond the False Negatives caused by functional equipment failures, measurement errors, and/or other unintentionally misapplied procedures, we should consider the failures intentionally produced by attacks to cyber-physical systems.

In [17] the discussion is focused on cybersecurity in the COVID-19 era, by highlighting the timeline and range of cyber-crimes and cyber-attacks experienced globally during this current pandemic. According to the analysis provided in this research, the COVID-19 also led to a

[5] https://www.immuni.italia.it/

[6] With a special relevance assumed by the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

secondary significant threat to a technology-driven society, that is both a series of indiscriminate and a set of targeted cyber-attacks and cyber-crime campaigns. Since the outbreak, there have been reports of scams impersonating public authorities and organisations, targeting support platforms as well as millions of people working from their own home, conducting Personal Protection Equipment (PPE) fraud and offering COVID-19 cures.

The increased use of remote working from home has led to a critical level of cybersecurity never reached before by industry and population. Cyber-criminals have used this opportunity to expand upon their attacks, using traditional techniques (i.e., malware, phishing, etc.), by pressing the feelings of fear, stress, anxiety and worry. In addition, the massive remote working revealed the general level of inadequacy and the lack of robustness of software products and the low readiness level of its vendors, particularly as far as the security of their products was concerned. Cyber-attacks have also targeted critical infrastructures such as healthcare services. So, it is therefore extremely challenging for organizations to develop appropriate protection and response measures given the dynamic environment.

Finally, another issue concerns the reliability and the quality of information that have been provided during the pandemic and its heavy weight on biasing public opinion and governance about the best practices, behaviors actions and policies to adopt.

[10] discusses on the fallibility of simulation models in informing pandemic responses, especially in the early stages of the COVID-19 pandemic, when mathematical models can provide valuable insights into transmission dynamics (e.g., see [9], help to predict disease spread, and evaluate control measures. In this work some limitations of the simulation models are highlighted, as the fact that models are only valid within the limits of the examined parameters, and the need to increase the sensitiveness of models to the changes occurring in their parameters. As reliable parameter estimates are rarely available early in a new pandemic, best-guess estimates are used, but they need to be constantly reviewed as new real-world data emerge, in order to provide useful information about validity when parameters are uncertain. These factors have to be considered in order to correctly interpret models without leading to flawed inferences, which can produce far-reaching effects when they inform public health policy and public opinion too.

Summing up, the COVID-19 pandemic raised remarkable and unique societal and economic circumstances, often and willingly leveraged by cyber-criminals, that utilized the event as a hook thereby increasing the likelihood of success for their attacks [13].

3 The big picture

Starting in the first half of 2020, several countries had to face an unprecedented crisis due to COVID-19. Two main macroscopic consequences were the fall of country productivity and political consequences of the management of the crisis, that in some cases caused political instability and oppositions reactions and anyway modified the political agenda and the structure of public expenses. For example, in some countries, like China and South Korea, massive personal tracking mechanisms have been introduced and limitations of personal freedom have been imposed to contain the spread of the virus, heavily affecting and changing the daily habits of citizens; in some countries, like Italy, restrictions have been imposed, weakening education because of the limitations to school attendance, limiting commerce and the industrial activity.

A role of paramount importance is played by information about infections, casualties and related dynamics. In a context in which there is no previous experience and existing models had to be reused with a few information about the specificity of the new virus, all decisions had to be based on partial, inhomogeneous and dirty data. A plurality of different voices dealt with the topic, amplified by media that served more or less prudentially as the main resource and guidance for the population. Official raw data have been collected and managed by the Istituto Superiore di Sanità, an official institution, and not disclosed to third parties. The government created a panel of experts that produced indications for the political action, on the basis of non-disclosed reports, raising criticisms and legal actions by the opposition. However, the role of data in the decision process that defines the immediate reactions of the country and impacts its next future is obvious.

3.1 A cyber warfare perspective

In general terms, the possibility of influencing the political equilibrium, the economy and, ultimately, the autonomy and the decisions of a foreign government are some of the targets of cyber warfare. Cyber warfare is the complex of military operations aiming at attacking foreign countries in the cyberspace, that is by leveraging information and communication technologies to reach and compromise military targets (e.g., critical infrastructures, information services, strategic technological platforms, economically relevant systems...) to obtain a benefit for own country or to damage the target country. The benefit might consist in a military advantage (taking over or destroying weapons or related resources or support/logistic chain, as in the Stuxnet case [18]), in gaining access to critical information systems for a useful period of time, in an image damage, in causing

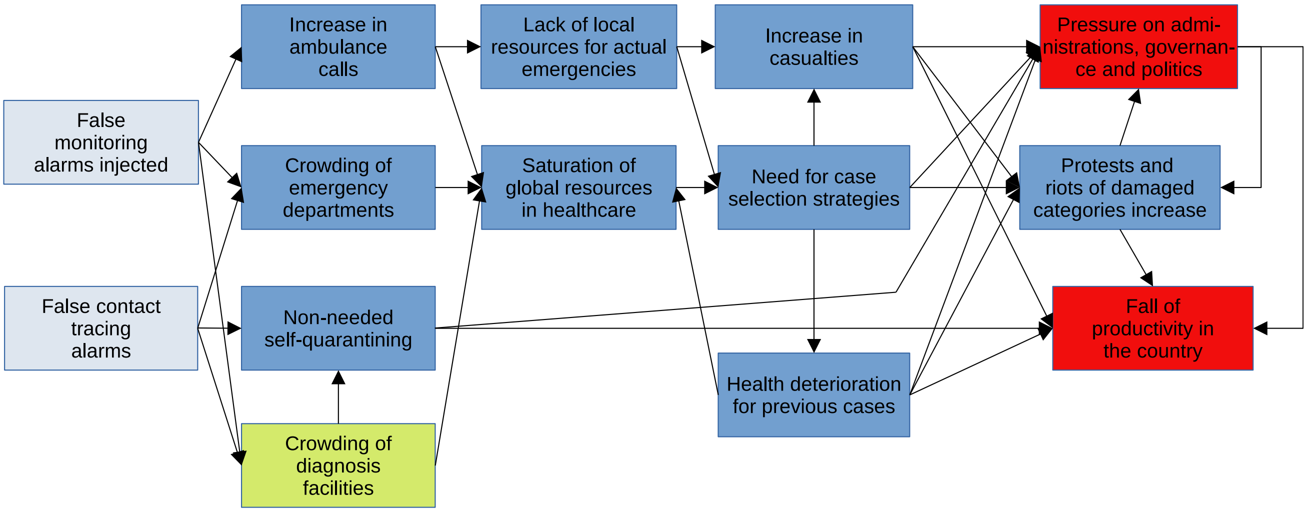
False monitoring alarms injected
False contact tracing alarms
Increase in ambulance calls
Crowding of emergency departments
Non-needed self-quarantining
Crowding of diagnosis facilities
Lack of local resources for actual emergencies
Saturation of global resources in healthcare
Increase in casualties
Need for case selection strategies
Health deterioration for previous cases
Pressure on admi-nistrations, governan-ce and politics
Protests and riots of damaged categories increase
Fall of productivity in the country

Fig. 1 Influence Net for the scenario

diplomatic cases, or in getting the devices to influence the economy (e.g., by supporting industrial espionage, or interfering with local industry to produce a tactical or strategical advantage on the market or in the international competition for own national competitors) and the politics of the target country (e.g., by disclosing confidential information that might destabilize the government or influence elections). In this perspective, the observed impact of COVID-19 on local economy and politics suggests that in similar situations gaining a leverage on the health system and the countermeasures of a target country might result in an influence on its economic competitiveness and political stability. While a direct impact seems to be beyond the possibilities of the cyber domain, the pervasivity of IoT technologies and smartphones in supporting contact tracing and personal health monitoring provides a viable tool to establish indirect influences, based on altering the signals that influence person and global decisions. In the following we will abstract from the specific case of COVID-19 pandemics to evaluate the viability of such a cyber warfare aggression strategies in similar cases at the current state of the technology.

3.2 Analysis of influences

In order to understand if, in principle, a cyber warfare activity based on proper coordination of cybersecurity attacks may impact at the desired macroscopic level, we analyzed the scenario with a qualitative technique inspired to Influence Nets [11]. The goal was to find a possible chain of consequences that may bind reachable technological targets to governance decisions or economic consequences. The model resulting from the analysis process is depicted in Fig. 1. A quantitative analysis of this model is out of the scope of this paper and is part of planned future work. Anyway, it is here important to point out that a quantitative analysis can provide an estimation of the impact of the chain of events and their influences on the selected events of interest in terms of likelihood by using an estimation of the weight of each influence (represented by an arc) produced by a panel of experts in different hypotheses.

The two technological targets that may be easily attacked, according to cited literature, are: *I)* - scarcely defended IoT sensors for critical or personal health monitoring and *ii)* - devices that host contact tracing applications, such as smartphones or publicly accessible access points: we assumed these two factors as independent events and evaluated other events on which their influence may be significant, as the attacks were performed according to a coordinated strategy. In both cases, given the possibilities of cyber warfare units, we derive the feasibility of the attack from two considerations. The first is based on the relatively small dimension of the market of common health-related IoT devices; the second on the fact that there is more diversity in smartphone and network devices than in the first case, but that in the most of the cases apps and updates are downloaded from a few sources. On this basis, cyber warfare units might gradually and partially gain control on the targets by exploiting a supply chain attack [20, 28], such as the one that significantly and visibly impacted USA targets in December, 2020[7] and was largely noticed by media. We denote the two related events as *False monitoring alarms injected* and *False contact tracing*

[7] No scientific reference is provided, as we write a few days after, but press documented the events, for example inhttps://eu.usatoday.com/story/news/politics/2020/12/18/russian-cyber-attack-worst-may-yet-come-solarwinds-hacking/3956223001/ .

alarms in Fig. 1. This chain of consequences is effective during a crisis, that is when the system is already solicited and close to maximum tolerable workloads, so that small influences may move the equilibria towards collapse and instability and produce the most disruptive effects possible.

We identified four main events that may be influenced by the two factors, namely:

- *Increase in ambulance calls*;
- *Crowding of emergency departments*;
- *No-needed self-quarantine*;
- *Crowding of diagnosis facilities*.

Increase in ambulance calls is a potential consequence of properly altering data collected by IoT sensors that are installed to monitor patients that are treated at home. This produces unnecessary calls for interventions, that cause ambulances and personnel to lose time and to become unavailable for real emergencies or for other needs.

Crowding of emergency departments is another consequence, due to reactions of patients that receive false alarms by their IoT devices or non-patients whose IoT non-medical monitoring devices or contact tracing systems signal a problem. This causes an overload on emergency departments, but also creates concentrations of people in which contagion is more likely, due to unsafe behavior of the people or lack of effective devices to keep safety conditions.

No-needed self-quarantine is caused, for short periods or until testing is possible and results are available, by contact tracing alerts in absence of symptoms. Self-quarantine may be imposed by the law, also as a consequence of recent simultaneous presence in the same place (e.g., an office, a restaurant, a public place, mass transport vehicles or stations...) with people signaled as positive or signaled, in turn, as contacted by contact tracing applications. This affects businesses, industrial production, commerce, services by temporarily forbidding part or all of the employees, that might have severe consequences on their economic sustainability during a crisis, in combination with other factors (e.g., lockdown effects). While self-quarantine lasts a short period, it is relatively easy to amplify its effects on specific targets or specific areas, as attacks may exploit real contact networks, leveraging subjects that actually have a large number of contacts per day (e.g., bus drivers on lines that cover densely inhabited areas of a city), and the alarmed people should warn all people that they have been actually or potentially in contact with independently from the contact tracing systems.

Crowding of diagnosis facilities causes inefficiencies and delays, and potentially lack of materials or personnel. As this is a potential bottleneck that affects the free employment of potentially positive people, we decided to perform a quantitative evaluation of the dynamics of a testing facilities and of the impact of false alerts on it in the next Section.

These events may in turn influence other ones, namely:

- *Lack of local resources for actual emergencies*;
- *Saturation of global resources in healthcare*.

Lack of local resources for actual emergencies raises the criticality of the effects of the attacks. If the attack manages to push the number of calls over the maximum coverage possible, additional personnel may be diverted from normal utilization in hospitals or similar facilities or may be forced to extra hours and stress. As additional personnel is not obviously and immediately available (and needs extra funds and training), this may severely affect the capabilities of the health system; in general, a *saturation of global resources in healthcare*, in terms of resources, personnel, devices may happen in the country, or in the most hit areas, and exceptional procedures and decisions may be needed; this situation paves the way for the most dramatic events caused in the chain, that are:

- *Increase in casualties*;
- *Need for case selection strategies*;
- *Health deterioration for previous cases*.

Increase in casualties results because of the excessive pressure on structures and personnel and on the consequent lack of time, attention or interventions that may be devoted to real cases, be it in hospitalized, home treated or chronically ill people or in case of actual emergencies. Such a pressure brings to errors, stress, tensions, mistakes that may make the situation even more pressing.

When critical resources and space are saturated, *need for case selection strategies* arises, causing doctors to choose between patients, delay surgery, change cures or procedures, send back home patients in difficult conditions to privilege subjects that have more chances, that naturally creates social tensions amplified by media. This also affects *increase in casualties* and causes *health deterioration for previous cases* that are not severe and would have stayed in the same or better conditions if the crisis did not divert resources: this, in turn, further affects *saturation of global resources in healthcare*.

Finally, the macroscopic consequences that have a systemic scope and are the events targeted by the leverages are:

- *Pressure on administrations, governance and politics*;
- *Protests and riots of damaged categories increase*;
- *Fall of productivity in the country*.

Pressure on administrations, governance and politics is of paramount importance to pilot strategic decisions, to influence elections and majorities, force participation in international agreements and in general to gain partial control of the reactions of target governments, including their fall, in extreme conditions. It is of course only one of the factors that may build power over target government, but it may be used to build a more complex strategy and as a leverage during negotiation processes or to induce to adhere to mutual exchanges or to desist from competition. *Protests and riots of damaged categories increase* is one of the reactions of public opinion, that may be solicited by propaganda built on top of restrictions and critical decisions. Raising the level of perceived severity of the crisis is a leverage, including the perception of a collapse of the health system, and a mutual influence exist with the *pressure on administrations, governance and politics* and resulting acts, that may start a self-sustained cycle of amplification of the effects in a spiral of overreactions. *Fall of productivity in the country* is a consequence of many factors, including the causes that are related to the permanent or temporary unavailability or limited effectiveness of workforce and the effects of protests, but is a primary target of a cyber warfare attack strategy. In fact, this event may hit the target country at many different levels. As first, the general economy of the country, already threatened by the crisis, might be damaged at the point that part of its structure collapses, its internal and global equilibria are compromised and a weaker economy will emerge as post-crisis equilibrium: strategic sectors might be targeted to substitute own presence over them in place of the one of the target country on the international level and on the global market. As second, the target may be the acquisition, by means of own finance or firms, of target country production assets at a price that is lower than the actual value, exploiting induced favorable conditions or exploiting the need for liquidity of target businesses. As third, target may be the general competitiveness of small firms in the target country, to give a push to own ones or to favor acquisitions or to start a substitution process by multinational firms. Resolutions of the target government may favor these effects as well, e.g., by limiting economic activity, workforce usage or business opportunities for safety reasons.

4 A quantitative insight on testing facilities

In order to model the behavior of the contact tracing system issued by governments in contrast to COVID-19 pandemic, we refer to Italian rules. It is to be kept in mind that these rules may differ from state to state, but the rules of other states may be modeled in a similar way.

The rules for management of symptomatic, positive and contact cases in Italy are stated by a circular letter of the ministry of October 12th, 2020 of *Ministero della Salute* (Ministry of Health)[8], in which are also stated the quarantine length and the need to carry out the swab. These rules state that the persons which have been in close contact with a patient tested as positive to COVID-19 must follow a quarantine period in two possible ways: (I) stay in quarantine for 14 days, and return to normal activities if in this period he manifests no symptoms, or (ii) stay in quarantine for 10 days, and return to normal activities after taking a negative swab.

In view of this, the behavior of the contact tracing system is detailed in the following:

1. The contact tracing system is alerted because a person has been found positive to COVID-19;
2. All close contacts of the subject must be alerted and invited to respect a quarantine period;
3. The quarantine period may be followed by close contacts by:
   (a) Staying in quarantine for 14 days and returning to normal activities if in this period they manifest no symptoms;
   (b) Staying in quarantine for 10 days, and returning to normal activities after they have carried out a negative swab;
4. If during the quarantine period (or after a swab) the subject is found infected by COVID-19, he must follow the insulation rules (different from quarantine).

This behavior is also shown in Fig. 2. The persons susceptible to infection (and not suspected to be infected) are in state *S*. When a person is alerted by the contact tracing system moves to state *Contact*. From this state, depending upon his choice, may evolve in state *Queue for swab* or in state *Wait 15d*. From state *Queue for swab*, the person, after having carried up a swab, may evolve in state *Infected* or returns to state *S*, depending on the results of the swab. From *Infected* the person, once he recovers from the disease (or if he passed away), evolves in the state *R or D*. We choose not to consider the case of a person which is recovered from COVID-19 disease and later infected again due to lack of data related to those cases.

The color codes used in Fig. 2 have the following meaning:

- Blue: normal activity state;
- Red: state of non-working person;
- Yellow: state of non-working person caused by real infection (unavoidable);
- White: transient state;
- Continuous lines: timed transition;
- Dashed lines: immediate transition.

[8] The circular letter may be found (in Italian) on *Ministero della Salute* web portal,http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioNotizieNuovoCoronavirus.jsp?lingua=italiano&id=5117 .

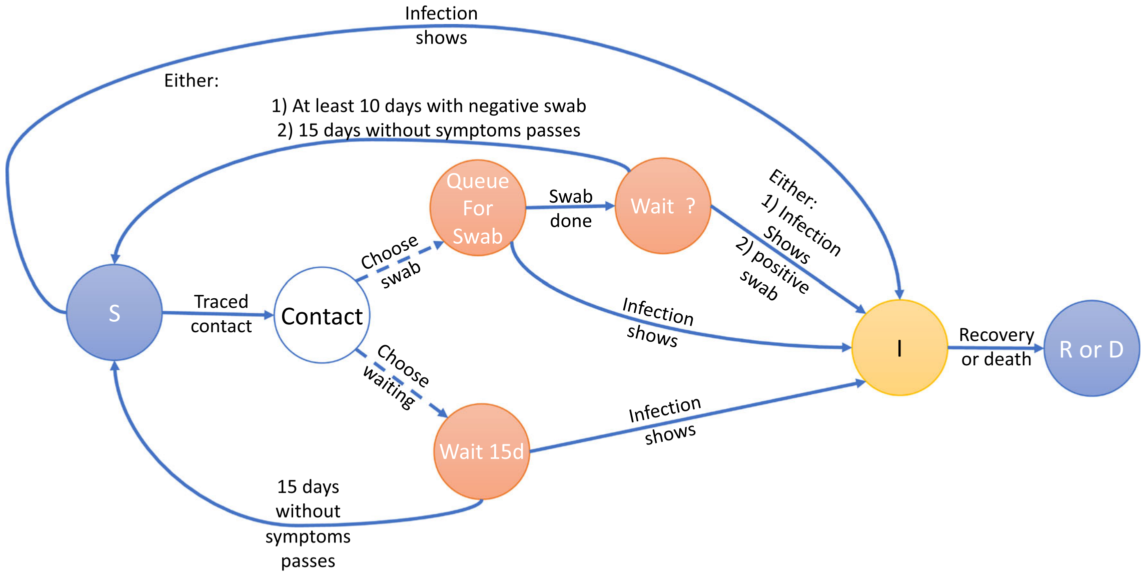

Fig. 2 Description of the behavior of the contact tracing protocol

5 A case study

We focus on a single geographical region, and model the considered system as a Markovian Agent Model (MAM [3]), composed by a single location. We use a Coloured Petri Net (CPN [14]) to describe the evolution of each agent with a high-level modeling language, and then we translate it to the corresponding MAM[9].

The considered CPN is shown in Fig. 3, where tokens can be of two colors: *Infected* (denoted with letter A and represented in red), and *Susceptible* (shown in blue, and identified by letter S). We use a graphical notation specified in the following.

Black primitives represent places, transitions and arcs that can be used by both types of tokens. In particular, each black transition can fire either in A or S modes, both modes characterized by the same firing rate (timed transitions) or weight (immediate transitions). When a transition fires in A mode, it removes and generates red tokens. Conversely, when it fires in S mode, it only uses and creates blue tokens. Red transitions and arcs, only fire using A tokens, while blue elements are limited only to S tokens. To simplify the picture, we also use *Broken Arcs*: arcs that ends on a small circle with a number written inside, continues from an identical spot in a different part of the picture.

To simplify the model, we consider the following assumptions:

- People can become infected only when they are in the *Susceptible* state (S in Fig. 2);
- We do not consider FP and FN in the results of a swab: a person modelled by an A token will always be detected as infected, and a S token will always produce a negative swab result;
- Infected people who have severe consequences and get identified by a medical intervention (such as a visit to and Emergency Department of an Hospital, or by the intervention of an ambulance) can jump directly to the infected state (I in Fig. 2). This can happen anytime: during the contact tracing, or before it, but only to infected people (A tokens);
- Infected people who have not been involved in the contact tracing process, or have decided not to proceed with a swab, and have not shown any symptom during the quarantine, will return to the susceptible state (S in Fig. 2) as infected token A. They might then show symptoms, or been involved again in another contact tracing, where they can again decide not to take a swab or wait another quarantine period.
- Although we have deterministic duration, such as the length of the quarantine, we approximate every duration with samples of an exponential random variables with the same average.

Place P_S represents the normal population: it includes both non-infected people (S tokens), and infected but undiscovered people (A tokens). Transition $T_{S->A}$ represents susceptible people that become infected: its action is to change color of tokens inside P_S from blue (S) to red (A). Its firing rate depends on the quantity of infected people in the system, as in conventional SIR model. Infected people (token color A) can have severe consequences that immediately show the infection (transition T_{I_1}), or can recover

[9] For other applications of CPN to these topics, see for example [4].

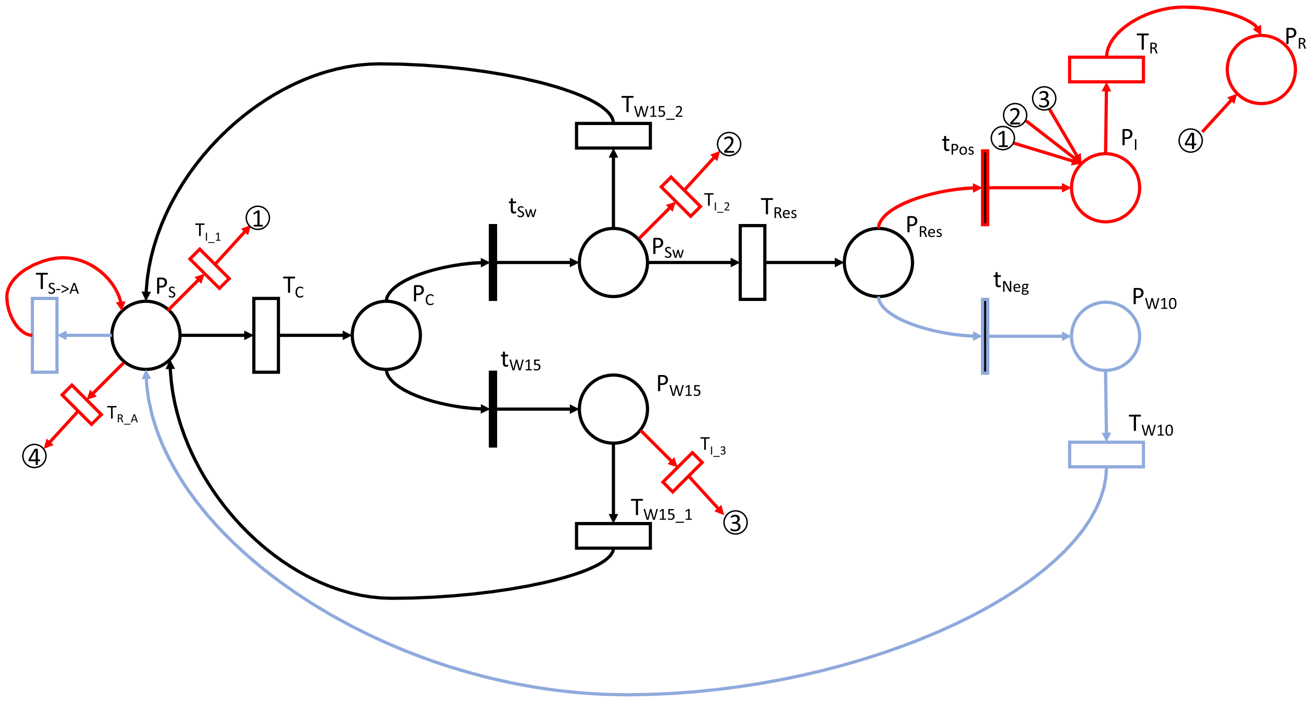

Fig. 3 The coloured Petri net model for the considered subsystems

autonomously without being discovered (transition T_{R_A}). Transition T_C represents the contact that can occur to a person, forcing him to chose either to wait for the quarantine, or the go for a swab. Place P_C models people making this decision: the choice of the swab is modelled by immediate transition t_{Sw}, and quarantine by transition t_{W15}.

Let us focus on the quarantine choice, represented by place P_{W15}. In this case, tokens wait the quarantine period, and if nothing happens, they return to be susceptible (Transition T_{W15_1}). Infected people (A tokens) can instead become severe and be identified, with the firing of transition T_{I_3}.

The swab execution is instead modelled by Place P_{Sw}, that represents the queue that people have to do before performing the test. If the time to perform the swab becomes larger than the quarantine time, people immediately return being susceptible, without performing the test (transition T_{W15_2}). As in the quarantine case, infected people can become severe and jump to the I state (Transition T_{I_2}). The queue for the execution of the test, is modelled by Transition T_{Res}, and the result of the test is modelled by place P_{Res}. Positive result is always taken for A tokens, by the firing of immediate Transition t_{Pos}. Negative swabs instead always occur for S tokens with immediate transition t_{Neg}.

Place P_I models the known infected people: their recovery is represented by the firing of Transition T_R. Place P_R models the recovered people, who now are no longer susceptible to the infection.

The negative result of the swab is modelled by Place P_{W10}, where S coloured tokens return to be susceptible according to the firing of Transition T_{W10}. The firing time of T_{W10} is chosen to approximate the behavior of the contact tracing protocol, that requires a shorter quarantine even for people who had a negative swab. In particular, it estimates the average time spent in place P_{Sw}, $\bar{t}_{Sw}$ using Little's law. Let us call $\bar{n}_{Sw}$ the average number of tokens in place P_{Sw}, and μ_{Res} the firing rate of transition T_{Res}. We approximate $\bar{t}_{Sw}$ as:

$$\bar{t}_{Sw} = \frac{\bar{n}_{Sw}}{\mu_{Res}} \tag{1}$$

Let us call $\mathcal{T}_{10}$ the length of the shorter quarantine period for people who did the swab, and ϵ a very short time period that we can use to approximate an immediate transition firing. We then define the firing rate μ_{W10} of Transition T_{W10} as:

$$\mu_{W10} = \begin{cases} \dfrac{1}{\mathcal{T}_{10} - \bar{t}_{Sw}} & \text{if } \bar{t}_{Sw} < \mathcal{T}_{10} - \epsilon \\ \dfrac{1}{\epsilon} & \text{if } \bar{t}_{Sw} \geq \mathcal{T}_{10} - \epsilon \end{cases} \tag{2}$$

The considered CPN model is a *Marked Graph* (see [19]), since every transition has exactly one input and one output arc. All transitions are *Infinite Server*, except Transition T_{Res}, which is single server, to model the queue that tokens might have to do for the swab.

5.1 The Markovian agent model

The CPN model shown in Fig. 3 is translated in the MAM shown in Fig. 4, where each place connected to a timed transition is transformed into one or two agent states, depending on the corresponding number of token colors, according to Table 1. The model has a total of nine agent states: we will define the average number of agents in a state as a vector $\mathbf{x} = |x_1, \ldots, x_9|$. The kernel matrix of the MAM evolution $\mathbf{R}(\mathbf{x})$, which describes the transition rate of the agent counts, is an infinitesimal generator matrix, whose nonzero entries are derived from the model parameters, defined in Table 2, and given in Table 3. Since the matrix is an infinitesimal generator, we have $r_{ij} = -\sum_{k \neq i} r_{ik}$. All rates depend on the state: the dependency has not been explicitly shown to simplify the notation. The initial state is defined as:

$$\mathbf{x}_0 = |S_0, A_0, 0, 0, 0, 0, I_0, 0, 0| \tag{3}$$

The evolution of the average number of agents in each state can be computed solving the following set of ordinary differential equation:

$$\begin{cases} \dfrac{d\mathbf{x}}{dt} & = & \mathbf{x} \cdot \mathbf{R}(\mathbf{x}) \\ \mathbf{x}(0) & = & \mathbf{x}_0 \end{cases} \tag{4}$$

Figure 5 shows the evolution of the average number of persons in each state. In particular curve labeled S shows the average number of susceptible persons ($x_1(t) + x_2(t)$, right axis), I the number of infected ($x_7(t)$ on the left axis) and R the number of recovered ($x_9(t)$ on the right axis). As we can see, there is a peak of infected around day 270, and after that the epidemic will start to decrease its spread. The figure also shows the evolution of the number of people waiting for a swab ($x_3(t) + x_4(t)$, curve Sw on the left axis) or waiting 15 days without a test ($x_5(t) + x_6(t)$, curve $W15$ on the left axis). As it can be seen, they reach their

Table 1 Correspondence between CPN Places and MAM states

Place	Variable
P_S	x_1 (for S tokens), x_2 (for A tokens)
P_{Sw}	x_3 (for S tokens), x_4 (for A tokens)
P_{W10}	x_5 (for S tokens), x_6 (for A tokens)
P_I	x_7 (A tokens only)
P_{W10}	x_8 (S tokens only)
P_R	x_9 (A tokens only)

Table 2 Model parameters

Param.	Description	Value
$\mathcal{T}_{10}$	Quarantine with swab	10 days
$\mathcal{T}_{15}$	Quarantine without swab	15 days
α	Contact rate parameter	0.001
β	Infection rate parameter	0.0001
γ	Recovery rate parameter	1/40
η	Detection rate parameter	0.005
p_S	Probability of taking a swan	0.5
μ_{Res}	Swab result rate parameter	1/3 days^{-1}
S_0	Initial number of susceptible population	10^6
A_0	Initial number of undetected cases	10^4
I_0	Initial number of infected cases	5000

Fig. 4 The MAM for the considered subsystems

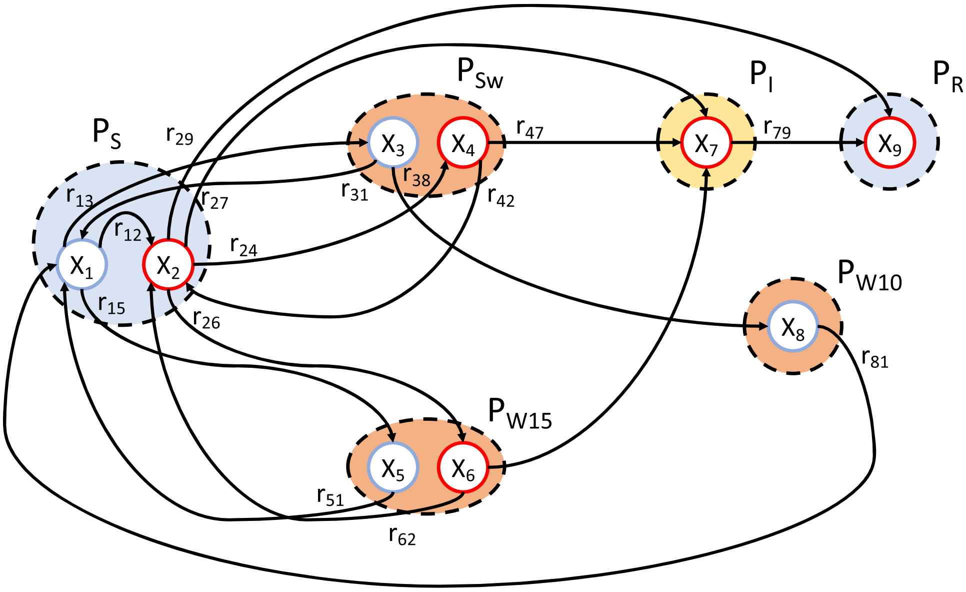

Table 3 MAM transition rates

Transition	Rate
r_{12}	$\beta \cdot (x_2 + x_4 + x_6 + x_7)$
r_{13}, r_{24}	$\alpha \cdot p_S$
r_{15}, r_{26}	$\alpha \cdot (1 - p_S)$
r_{27}, r_{67}	η
r_{29}, r_{79}	γ
r_{31}, r_{51}, r_{42}, r_{62}	$1/\mathcal{T}_{15}$
r_{38}	$\frac{\mu_{Res}}{x_3 + x_4}$
r_{47}	$\frac{\mu_{Res}}{x_3 + x_4} + \eta$
r_{81}	Equation 2 with $\bar{n}_{Sw} = x_3 + x_4$

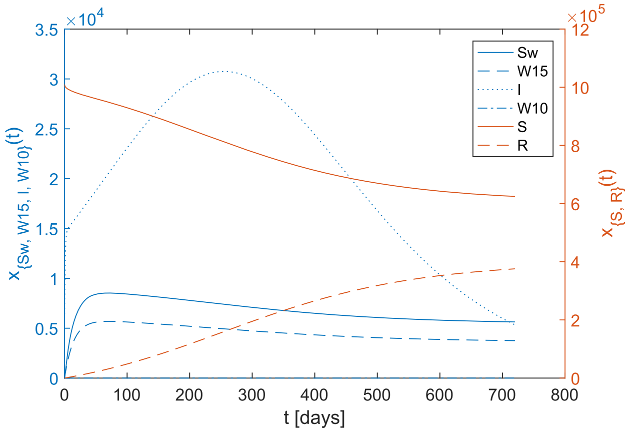

Fig. 5 The evolution of the average number of people in the considered states

maximum in about one month, and then they remain almost stable, with a very slow growth. The picture also shows the number of people waiting 10 days with a negative swab ($x_8(t)$, curve $W10$ on the left axis) is negligible: this is caused by the fact that the swab system saturates almost immediately, making very unlikely to have results earlier than 10 days.

Figure 6 shows the effect of the contact rate α, ranging from one contact every 1000 days to one contact per day, on both the evolution of the infection, and on the average time people stays in quarantine W three months after the beginning of the spread ($t = 90$ days). In particular, W is computed using Little's law, starting from the instantaneous throughput $\bar{X}$ and the average blocked population N, computed respectively in the following ways:

$$\bar{X} = \frac{x_3(t) + x_5(t)}{T_{15}} + \frac{x_8(t)}{T_{10}} \tag{5}$$

$$N(t) = x_3(t) + x_5(t) + x_8(t) \tag{6}$$

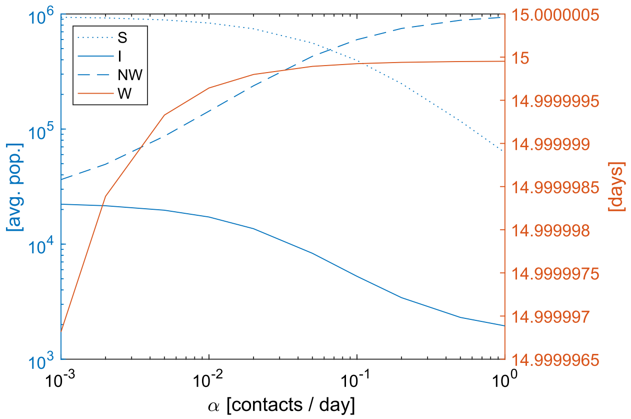

Fig. 6 Susceptible, Infected, total population at home, and average waiting time as function of the contact rate α

$$W(t) \approx \frac{N(t)}{\bar{X}(t)} \tag{7}$$

The figure also shows the total number of people not working $NW(t) = \sum_{I=3}^{8} x_i(t)$. As it can be seen, the average waiting time W is almost constant and independent from α: this is because, as outlined, the swab system saturates almost immediately, leaving all persons waiting the full 15 days at home before resuming their activities. It is interesting to see the positive effect of increasing the contact tracing procedure has in reducing the infection: the more frequently people are tested, the less likely the infection will spread, with a reduced number of infected I, this however at the cost of having a very rapidly increasing number of not working people NW. In the worst possible scenario, where everybody is put in quarantine after around one day of normal activity ($\alpha = 1$), basically all the susceptible population (curve S) is in quarantine at the considered day.

5.2 The effect of false positive injection

It is interesting to investigate on what happens in case of false contact tracing alarms. Almost all contact tracing apps (CT) record the proximity of single persons using Bluetooth [1], and provide an alert if one of the contacts of that person is registered in the positive people database. Due to privacy constraints, many EU CT apps update their own database when an (anonymous) user, resulting infected, sends an alert. The CT apps are installed on regular smartphones, and are obviously much easier to attack than servers; an attacker may choose to hack a user's smartphone, sending the alert: all the recent contacts of that user are alerted, and are subject to quarantine, as modeled above.

Determining the mean number of contact of a generic user is not an easy task, depending on his job, social customs, lifestyle etc.. In [21] information obtained using cross-sectional surveys conducted in different EU countries is analyzed. In the investigation, the mean number of contacts grouped by age, household size, day of the week, and country is shown. The higher contact number is - not surprisingly - found in Italy, with a mean of 19,77 contacts per person, which is used as a starting point in our analysis. On the other side, this number is drastically reduced due to lockdown measures, as shown in [7], so in this work the number of 8 as mean contacts per person is used.

In case of FP injection, the total number of quarantined persons (Qtot) is:

$$QTot = TP * MNC + FP * FNC \tag{8}$$

where TP is the number of True Positives (TP), MNC is the mean number of contacts per person (in this study, $MNC = 8$), FP is the number of false positives (injected by attacker) and FNC is the number of the contacts of FP. It is evident that, if FNC is of the same order of magnitude of MNC, an attacker needs to hack a big number of smartphones to cause serious damage, so a casual smartphone attack has limited effects. However, if FNC is much bigger than MNC, the situation will change. In Fig. 7 the trend is shown of the ratio $QTot/QTot0$, where $QTot0$ is the number of quarantined persons in case of no FP. On the horizontal axis the ratio of FP/TP in percentiles is displayed. The three displayed lines are the cases: (I) $FNC = 10 * MNC = 80$; (ii) $FNC = 50 * MNC = 400$; and (iii) $FNC = 100 * MNC = 800$.

Looking at Fig. 7 it is evident that, in case $FNC > > MNC$, the effect on the total quarantined persons is amplified. As an example, consider a little city in which there are 300 TP per day. Attacking less than 2% of TP will cause a doubling of quarantined persons, if the contact number of FP is 400. This case is not so rare: bus drivers are near a big number of persons during the whole work day, and a single bus may contain $50 - 100$ persons per route; a checker of a supermarket meets many persons too.

A possible effective attack strategy may concentrate the efforts in hacking the smartphones of those particular workers, or, in alternative, an attacker may use his own smartphone to meet the maximum number of persons in a few days, and, after, signaling himself as a positive. The defense measures must take into account those issues, considering to provide those categories of workers a secure smartphone, and to carefully monitor the case of positives with a large number of contacts.

6 Conclusions and future work

State estimation of a system is crucial to provide operators with situational awareness and is used by several applications, like contingency analysis, power markets and healthcare, among the others. Several researches in the past have highlighted the vulnerability of state estimators to stealthy false data injection attacks that bypass bad data detection mechanisms. Adopted mitigation strategies either focus on masking the effect of attacks through redundant measurements or prevent attacks by increasing the cybersecurity of associated sensors and communication

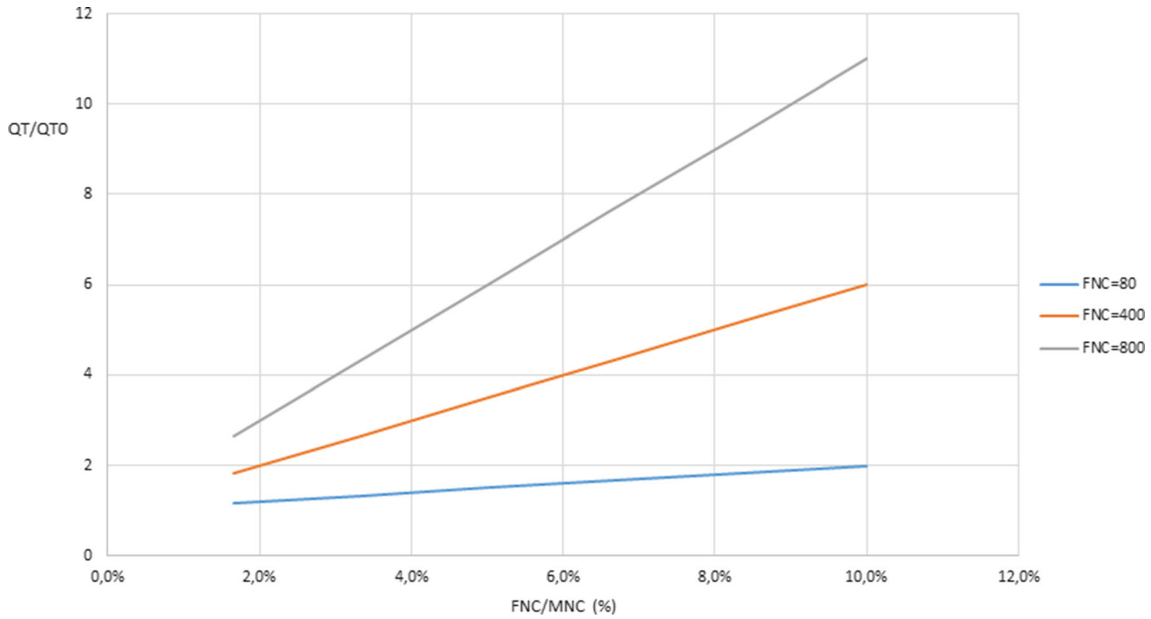

Fig. 7 Growth of total quarantined persons in function of false positives

channels. However, this kind of offline approaches put too specific assumptions about the nature of target systems and attacks, making them often too restrictive and grossly inadequate to deal with dynamically evolving cyber threats and quickly changing configurations of systems.

Detection of abnormal behaviors is essential in complex and/or strategic systems requiring reliability, safety and security. Ensuring that sensing devices are not operating out-of-specifications is highly useful in detecting anomalies caused by physiological elements of failure to a system or intentional malevolent actions. In this regard, digital sensors are particularly attractive as they are portable and easy to calibrate; however, they exhibit the property of considering the operating environmental conditions altogether, as a whole, without a precise knowledge about each. This property endows digital sensors with fewer FP when compared to analog sensors. So, in this work we analyzed the possibility of a massive targeted use of health-oriented IoT devices and smartphones as vectors for cyber warfare operations during future crises that resemble the current COVID-19 one. We provided a qualitative analysis of the chain of consequences that may make similar external influences viable to alter economic and political equilibrium, and a quantitative analysis of the possible effects on a subsystem of the overall reaction and management apparel, namely the complex of the testing facilities, that shows how such influence may be used to reduce the availability of workforce and the activity of small business.

Increasing contact tracing by means of personal and fixed digital sensors may significantly help to control the diffusion of the contagion, but presents privacy problems and opens vulnerabilities that may enable escalations and a systemic impact on the society, which severity depends on the type and target of the attack and on the nature and prescriptions of the disease: consequently, quantitative studies and impact analysis by chains of consequences and course of events should be carried on and considered, as well as a higher attention level on connected embedded systems and IoT devices and commodities must be kept since the first stages of the design, development and deployment process, to protect the systems and the society by implementing security by design approaches.

As this paper is presenting a preliminary analysis and the effects on a subsystem, future work is planned about a quantitative evaluation of the global effects of the presented chain of consequences by Timed Influence Nets, when enough quantitative information will be available in literature or from expert panels, together with the analysis of other subsystems and a global, multiformalism modeling based, quantitative analysis.

Acknowledgments One of the authors (A.B.) has been supported by the Università del Piemonte Orientale, Italy. This work has been partially funded by the internal competitive funding program "VALERE: VAnviteLli pEr la RicErca" of Università degli Studi della Campania "Luigi Vanvitelli" and by project "Attrazione e Mobilità dei Ricercatori" Italian PON Programme (PON_AIM 2018 num. AIM1878214-2).

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Ahmed N, Michelin RA, Xue W, Ruj S, Malaney R, Kanhere SS, Seneviratne A, Hu W, Janicke H, Jha SK (2020) A survey of covid-19 contact tracing apps. IEEE Access 8:134577–134601
2. Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of things security: a survey. J Netw Comput Appl 88:10–28
3. Bobbio A, Cerotti D, Gribaudo M, Iacono M, Manini D (2016) Markovian Agent Models: A Dynamic Population of Interdependent Markovian Agents. Springer International Publishing, Cham, pp 185–203
4. Chang E, Moselle KA, Richardson A (2020) Covidsimvl – transmission trees, superspreaders and contact tracing in agent based models of covid-19. https://www.medrxiv.org/content/10.1101/2020.12.21.20248673v1
5. Cho H, Ippolito D, Yu YW (2020) Contact tracing mobile apps for covid-19: privacy considerations and related trade-offs. https://arxiv.org/abs/2003.11511
6. Dong Y, Yao YD (2020) Iot platform for covid-19 prevention and control: a survey. https://arxiv.org/abs/2010.08056
7. Eilersen A, Sneppen K (2020) Cost-benefit of limited isolation and testing in covid-19 mitigation. Sci Rep 10(1):1–7
8. Flaxman S, Mishra S, Gandy A, Unwin HJT, Mellan TA, Coupland H, Whittaker C, Zhu H, Berah T, Eaton JW et al (2020) Estimating the effects of non-pharmaceutical interventions on covid-19 in Europe. Nature 584(7820):257–261
9. Gribaudo M, Iacono M, Manini D (2021) COVID-19 spatial diffusion: a Markovian Agent-based model. Mathematics. https://doi.org/10.3390/math9050485
10. Gurdasani D, Ziauddeen H (2020) On the fallibility of simulation models in informing pandemic responses. The Lancet Global Health 8(6):e776–e777
11. Haider S, Levis AH (2008) Modeling time-varying uncertain situations using dynamic influence nets. Int J Approx Reason 49(2):488–502. https://doi.org/10.1016/j.ijar.2008.04.007
12. Hellewell J, Abbott S, Gimma A, Bosse NI, Jarvis CI, Russell TW, Munday JD, Kucharski AJ, Edmunds WJ, Sun F et al (2020) Feasibility of controlling covid-19 outbreaks by isolation of cases and contacts. The Lancet Global Health
13. Interpol (2019) Cybercrime: Covid-19 impact. https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf
14. Jensen K, Kristensen LM (2009) Coloured petri nets: modelling and validation of concurrent systems, 1st edn. Springer Publishing Company, Incorporated
15. Kamal M, Aljohani A, Alanazi E (2020) Iot meets covid-19: status, challenges, and opportunities. https://arxiv.org/abs/2007.12268
16. Lai S, Zhou NRL, Prosper O, Luo W, Floyd J, Wesolowski A, Santillana M, Zhang C, Du X, Yu H, Tatem A (2020) Effect of

non-pharmaceutical interventions to contain covid-19 in china. Nature 585(7825):410–413

17. Lallie HS, Shepherd LA, Nurse JR, Erola A, Epiphaniou G, Maple C, Bellekens X (2020) Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic
18. Langner R (2011) Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur Priv 9(3):49–51
19. Marsan MA, Balbo G, Conte G, Donatelli S, Franceschinis G (1994) Modelling with Generalized Stochastic Petri Nets, 1st edn. Wiley, USA
20. McFadden F, Arnold R (2010) Supply chain risk mitigation for it electronics. In: Supply chain risk mitigation for IT electronics, pp 49–55
21. Mossong J, Hens N, Jit M, Beutels P, Auranen K, Mikolajczyk R, Massari M, Salmaso S, Tomba GS, Wallinga J et al (2008) Social contacts and mixing patterns relevant to the spread of infectious diseases. PLoS Med 5(3):e74
22. Muheidat F, Tawalbeh M, Quwaider M, Saldamli G et al (2020) Predicting and preventing cyber attacks during covid-19 time using data analysis and proposed secure iot layered model. In: 2020 Fourth International Conference on Multimedia Computing. Networking and Applications (MCNA), IEEE, pp 113–118
23. Mulder T (2019) Health apps, their privacy policies and the gdpr. Eur J Law Technol
24. Psychoula I, Chen L, Amft O (2020) Privacy risk awareness in wearables and the internet of things. IEEE Pervas Comput 19(3):60–66. https://doi.org/10.1109/MPRV.2020.2997616
25. Saheb T, Izadi L (2019) Paradigm of iot big data analytics in the healthcare industry: a review of scientific literature and mapping of research trends. Telemat Inform 41:70–85
26. Singer PW, Friedman A (2014) Cybersecurity and cyberwar: what everyone needs to know. Oxford University Press, USA, New York
27. Ukil A, Bandyoapdhyay S, Puri C, Pal A (2016) Iot healthcare analytics: the importance of anomaly detection. In: 2016 IEEE 30th international conference on advanced information networking and applications (AINA), IEEE, pp 994–997
28. Wu M, Song Z, Moon YB (2019) Detecting cyber-physical attacks in cybermanufacturing systems with machine learning methods. J Intell Manuf 30(3):1111–1123