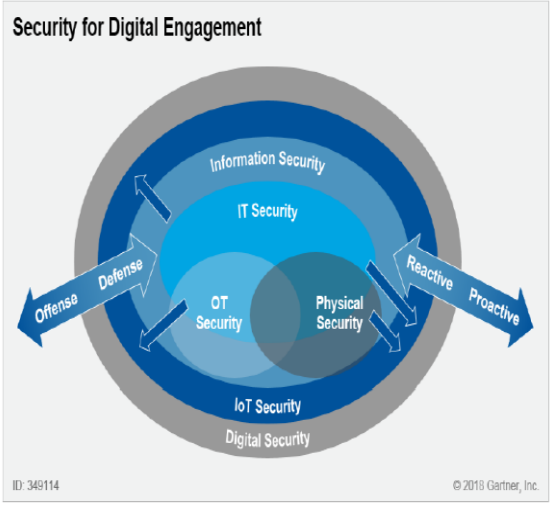
resource owners and decisions are consistently based on information and consideration.The research highlighted here gives CIOs guidance they need to succeed in this complex environment.

Definition: Digital risk management is the integrated management of risks associated with digital business components, such as cloud, mobile, social, big data, third-party technology providers, OT and the IoT [1].

Technology risk and how to confront it is now a permanent reality that operational and strategic leaders must fully comprehend. Technological risk is no longer simply the narrow concern of technical professionals. Exposure to risk is no longer felt only in small delays or malfunctions. The evolution of business into an activity defined by digital engagement brings technology risk closer to an organization's actions and decisions. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day, often without realizing the significance of what they're doing. The consequences of these choices can be calamitous, just as the potential of digital business constantly grows. The CIO becomes the central agent stressing the connections between business and digital risk — connections that should be important to technical and nontechnical staff, from contributor-level staff to the board. This is a moment for CIOs to be deliberate in their implementation and communication of digital risk management issues with all of the participants in the business. With staff prioritizing the organization's measured consideration of its business plan and environmental factors, the enterprise will be positioned to cover external threats, economic conditions, social attitudes, political changes and regulatory requirements. (See Figure 1 for a depiction of interrelated security.)



Source: Gartner (January 2018)

Figure 1
Security for Digital Engagement

CIOs can engage the entire enterprise in digital risk management efforts, changing perceptions of risk enable the organization to better operate with informed decision making.

2.2Cybersecurity and Cyber Defense

Cybersecurity and cyberdefense remain ill-defined and inconsistently applied concepts and the policy documents produced remain vague on specific policy details and solutions. An important reason for this vagueness is a lack of consistent or defined nomenclature. There are several national conceptualizations and definitions published by state policies and strategies, conceptualizations as diverse as the national perspectives and priorities they reflect. While “cybersecurity” is a popular term in the media, policy jargon and civilian discourse, several states substitute “digital” for “cyber” while still referring to the same issues as their international partners. At one level this is to be expected. With the establishment of a policy-development framework which incorporates all interested government parties – military and non-military alike – a government will subsequently have the expertise in place to ask: what are the main cybersecurity risks and how does we mitigate them? A systemic consequence of this process, however, is that national priorities, path dependencies and vagaries in national political and strategic culture inevitably play a role in defining cybersecurity and cyberdefense.This lack of standardized nomenclature creates difficulties for analysis as well as contributing to the overall conceptual and definitional fog which continues to surround cybersecurity and cyberdefense [4, pp. 80-81).

There are two further consequences of this tendency to build organizational structures before developing policy. The first is an observable trend towards centralizing leadership and oversight in cybersecurity and cyberdefense. This is being carried out to reduce the fragmentation of responsibilities and remits and streamline both policy development and operational processes. The second is that, when centralized structures and frameworks of co-operation are established, oversight and leadership responsibilities for both cybersecurity and cyberdefense tend to gravitate towards non-military – i.e. civilian – ministries, offices, agencies and bureaux. For cybersecurity this makes logical sense given that most of the malicious cyber activity is criminal in nature.

However, for cyberdefense this gravitation away from military leadership and oversight is somewhat unexpected given the national security rhetoric surrounding it.

Even in those few examples where intelligence and military agencies have operational oversight of cyberdefense – such as the UK – the agencies themselves fall under the aegis of foreign or interior ministries and not defense ministries. Furthermore, overall leadership in this sector stems from civilian entities. For both cybersecurity and cyberdefense this demonstrates a trend towards holistic, civilian oversight of these policy areas, despite the strong interconnection of cyberdefense with national security and defense strategy [4, p. 80].

Due to the ever-increasing availability and variety of sophisticated malicious digital tools and the ease with which these tools can be deployed, cybersecurity is now a crucial element of national security. Within this larger context, the concept of cyberdefense, with its implicit military connotation, has also gained significantly more prominence.

National policies of the kind analyzed in the snapshots contained in this collection define these concepts very differently. However, in order to conduct an effective examination and analysis of national policy a set of base-line definitions is needed.

As working definition, we understand cyberdefense to fall under the purview of a country's national security policy, and therefore is a part of its defense department or ministry, while nevertheless retaining a close a link to the overall policy efforts to improve a country's cybersecurity. As such cyberdefense intersects with cybersecurity [4, p. 4].

Cybersecurity policies tend to be more holistic and are released into the public domain, with references to ensuring civilian that infrastructures such as banking and personal computer networks are secure and resilient to cyber intrusions and setting out measures designed to tackle online criminal activity (cybercrime).

Cyberdefense by contrast is more of a closed box. This is due to its close relationship to secret, classified aspects of government policy and activity1.

As such, cyberdefense deserves special attention in studies of national policy such as this collection of analyses and is treated separately in the policy snapshots contained in this collection. Since there is an overall impression that the risks to national security from cyberspace have changed both in terms of quantity (more incidents are occurring) and quality (these incidents are becoming more sophisticated), many states have re-evaluated their previous cybersecurity efforts. In the ten years to 2018 many national policies and strategies have been published specifically addressing cybersecurity and cyberdefense.

Although these policies and strategies address similar issues, there is significant variation in approaches given national priorities and conceptualizations of the issues at hand [4, p. 4]. Cybersecurity and cyberdefense are constantly shifting and evolving topics. The technology used to carry out cyberattacks, and the tools required to mitigate or deter those attacks, is in a constant state of development and innovation. As a result, national policy relating to these topics also undergoes periodic shifts and changes, depending on national priorities [4, p. 6].

There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international organizational statements [7].However, [3] gives definition and further explanation of term cyberdefense as follows: Cyber defense is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks.

Cyber defense focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. With the growth in volume as well as complexity of cyberattacks, cyber defense is essential for most entities in order to protect sensitive information as well as to safeguard assets.Cyber defense provides the much-needed assurance to run the processes and activities, free from worries about threats. It helps in enhancing the security strategy utilizations and resources in the

most effective fashion. Cyber defense also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations.

By the recognition of the need to accelerate detection and response to malicious network actors, the United States (US) Department of Defense (DoD) has defined a new concept, Active Cyber Defense (ACD) as DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities [5].

3 Cybersecurity Strategy and Risk Management

While the cost of defending cyber structures as well as the payoffs from successful attacks keeps rising, the cost of launching an attack simultaneously keeps decreasing [8].

The key to increasing cybersecurity is getting to lower levels of vulnerability. Although threat awareness is important, by reducing vulnerabilities, all attacks are made more difficult [6].

3.1 Cybersecurity Risk Management

If there isn't sufficient visibility of cyber security status, organizations won't be able to manage cyber security risks and they will almost certainly suffer a breach. "Visibility of cyber security status" means having the complete picture, with measurements so that we can answer the following questions:

- What are our current measured levels of cyber security risk across the Enterprise from the multiple threats that we face?
- Are these cyber security risks tolerable?
- If not, what is our justified and prioritized plan for managing these risks down to tolerable levels?
- Who is responsible and by when?

The ability to measure cyber security status is fundamental; if we can't measure then we can't manage. Security incident and event management (SIEM) and data analytics solutions can provide valuable indications of actual or potential compromise on the network, but these are partial views, indicators of our overall risk status but not measurements of our risk status.

Similarly, threat intelligence services can identify data losses and provide valuable indications of actual or impending attacks but again these are not measurements of our risk status. The same can be said individually about outputs from compliance management, vulnerability management, penetration testing and audits.

Only by pulling together all the relevant indicators and partial views can we develop overall risk-based measurement and visibility of our cyber security status [9]. When confidence in our cybersecurity risk measurements exists, it is possible to respond to events and make decisions quickly, e. g.:

- Be able to identify risks that we aren't prepared to tolerate and have a clear and prioritized risk-based action plan for the control improvements necessary to reduce these risks to an acceptable level
- To have a better understanding of the implications from threat intelligence or outputs from SIEM and data analytics allowing faster, better targeted responses
- To develop risk-based justifications for investment in cyber security solutions and services.

But with the very high level of threat and high rates of change in both the threat and control landscapes we need to be able to refresh our view of our cyber security status on an almost daily basis.

Cybersecurity risk management which previously might have been an annual process as part of planning and budgeting is now a critical real-time facilitator in the battle against cyber breaches [9]. Cyber security breaches occur when people, processes, technology or other components of the cyber security risk management system are missing, inadequate or fail in some way. So, we need to understand all the important components and how they inter-relate.

This doesn't mean that risk management system needs to hold details of (for example) every end point and the status of every vulnerability on the network because there are other tools which will do that but the risk management system does need to know that all end points on the network have been (and are being) identified and that critical vulnerabilities are being addressed quickly.

Cybersecurity success is essentially the result of an effective risk management process. However, this process is being challenged by the inherent complexity of systems, developed with vulnerable components and protocols, and the crescent sophistication of attackers, now backed by well-resourced criminal organizations and nations.

3.2 Known Knowns, Known Unknowns and Unknown Unknowns

Although unknown unknowns may be unidentifiable, they might be presumed likely in some component of the system. A likely event cannot be thought to be unknown unknown because

it is already identified, but its consequence may fall into the category of unknown unknowns.The occurrence of an event like a natural disaster may be forecasted easily, but its impact is not easy to predict or estimate because of knock-on effects.Despite that project risk management acts as"forward-looking radar" it is not possible to identify all risks in advance, in part for the following reasons:[2]

- Some risks are inherently unknowable.
- Some risks are time-dependent.
- Some risks are progress-dependent.
- Some risks are response-dependent.

A typical classification of risks is based on the level of knowledge about a risk event's occurrence (either known or unknown) and the level of knowledge about its impact (either known or unknown). This leads to four possibilities:

- Known–knowns (knowledge),
- Unknown–knowns (impact is unknown but existence is known, i.e., untapped knowledge),
- Known–unknowns (risks), and
- Unknown–unknowns (unfathomable uncertainty). (Cleden, 2009)

The proposed model modifies and extends these categories to incorporate insights from the literature. This is discussed in the next section, which also explains how to use the model to identify hidden uncertainties and shows how recent catastrophes can be mapped to the model.

Figure 2 shows a schematic structure of the risk categorization. In this table, the model categorizes events by "identification" and "certainty."

Certainty / Identification	Certain (Known)	Uncertain (Unknown)
Identified (Known)	Known known (identified knowledge)	Known unknown (identified risk)
Unidentified (Unknown)	Unknown known (untapped knowledge)	Unknown unknown (unidentified risk)

Figure 2
Schematic Structure of Modified Risk Categorization

In this matrix, if the nature of an event is certain, it is more like a fact or knowledge. It could be what we already know, i.e., known known, or what we don't know yet, i.e., unknown known. If the nature of an event is uncertain, the occurrence can be uncertain, i.e., probability of occurrence is less than 1, and the impact can be uncertain as well. For example, a hurricane has two basic uncertainties. One is track, represented by the chance of landfall, and the other one is intensity, represented by wind speed or hurricane category. If either one of occurrence or impact is uncertain, that event is considered to be uncertain. Often, people know the identity of an uncertain event, which means known unknown. Sometimes, people even don't know what that is, which means unknown unknown. Most natural disasters are uncertain events, but people already know what they are.

Once identified, an unknown unknown is converted to a known unknown and moved to the quadrant at the right top in this matrix. Converting unknown unknowns to known unknowns means reducing the number of unidentified uncertainties even though we don't know how many of them are still remaining unidentified. The more unknown unknowns are identified, the less chance a project will have to be affected by a surprise [2].

3.3 Cyber Resilience

With this scenario of uncertainties and high volume of events, it is essential the ability of cyber resilience. Cyber resilience is the ability of a system, organization, mission, or business process to anticipate, withstand, recover from, and adapt capabilities in the face of adversary conditions, stresses, or attacks on the cyber resources it needs to function. Cyber resilience from an organizational perspective is defined as "the ability to continuously deliver the intended outcome despite adverse cyber events", and this definition is systematically described and justified [10].

Starting with the 2012 World Economic Forum meeting in Davos, cyber resilience [10] has been not only an area of growing importance for individuals, businesses and societies, but also a concept that has gained in attention and usage.

Cyber resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. The notion of continuously, means that the ability to deliver the intended outcome should be working even when regular delivery mechanisms have failed, during a crisis and after a security breach. The notion also denotes the ability to restore the regular delivery mechanisms after such events as well as the ability to continuously change or modify these delivery mechanisms if needed in the face of changing risks. The intended outcome refers to that which the unit-of-analysis (e.g. the nation, organization or IT system) is intended to achieve, such as the goals of a business or business process or the services delivered by an online service [10].

4 Resilience in Information-Communication Environment

Cybersecurity is an inherently distributed problem that will continue to evolve at the speed of technology. According to the 11th Annual Global Information Security Survey, conducted by PriceWaterhouseCoopers and CSO Online [11], executives remain confident in the robustness of their security initiatives.

In the survey, 84% of CEOs and 82% of CIOs contend their cyber security programs are effective, while 78% of chief information security officers express full confidence in their existing cyber security programs. With breaches on the rise, companies should focus on cyber resilience, not just cyber security. The number of security incidents detected is rising significantly year-over-year – climbing from 2,989 reported in 2012 to 3,741 in 2013.

Add to that the fact that the average losses per incident are up 23% year-over-year, and that the number of organizations reporting losses of more than $10 million per incident is up 75% from just two years ago [12].

Cyber security isn't going far enough so Cyber Resilience must be taken into consideration. Once businesses accept that cyberattacks will be made against their organizations and will be successful, they can move to the next step: implementing a Cyber Resilience Program (CRP). A CRP encompasses the ideas of defense and prevention but goes beyond those measures to emphasize response and resilience in moments of crisis [12].

4.1 Information Security, Cybersecurity and Cyber Resilience

Cybersecurity is no longer enough: there is a need for strategy of defense, prevention and response. The idea of resilience, in its most basic form, is an evaluation of what happens before, during and after a digitally networked system encounters a threat. Resilience should not be taken to be synonymous with "recovery". It is not event-specific: it accrues over the long term and should be included in overall business or organizational strategy.

Resilience in context of ability of systems and organizations to withstand cyber events means the preparations that an organization has made with regard to threats and vulnerabilities, the defenses that have been developed, and the resources available for mitigating a security failure after it happens. Normalization is key. Cyber risk should be viewed just like any other risk that an organization must contend with in order to fulfill its goals. Leaders of business and government need to think about resilience for two reasons: first, by doing so they avoid the catastrophic failure threatened by an all-or-nothing approach to cyber risks (i.e. preventing network entry as the only plan), and second, it ensures that the conversation goes beyond information technology or information security [13].

The first point, that a long-term view and durability are key factors in ensuring cyber resilience, does not need further explanation. A plan that encompasses actions and outcomes before, during and after the emergence of a threat will generally be superior to a plan that only considers one instance in time. The second point, that leaders must broaden the conversation, merits more attention. It is vital to our economic and societal resilience that we think beyond information security to overall network resilience that ensures we can deal with existing risks and face new risks that will come with such things as artificial intelligence, the internet of things or quantum computing. In order to ensure long-term cyber resilience, organizations must include in their strategic planning the ability to iterate based on evolving threats from rapidly evolving disruptive technologies [13].

By promoting an overall cyber resilience approach, long-term strategy (including which technologies a business will implement over the next five, 10 or more years) is a continual strategic conversation involving both technology and strategic leaders within an organization. The cyber resilience approach ensures greater readiness and less repetition – making it, on the whole, more efficient and more effective. Security, in contrast to resilience, can be seen as binary. Either something is secure, or it isn't. It is often relegated to a single, limited technical function, keeping unauthorized users out of a networked system [13].

While there are many broader definitions of cybersecurity, there is a difference between the access control of cybersecurity and the more strategic, long-term thinking cyber resilience should evoke. Additionally, since vulnerability in one area can compromise the entire network, resilience requires a conversation focused on systems rather than individual organizations. For networked technologies, vulnerability in one node can affect the security and resilience of the entire network. Therefore, resilience is best considered in the context of a public good or "commons". That's why partnerships are key. These can be between businesses as well as with regulators, prosecutors and policymakers [13].

Since cyber resilience is really a matter of risk management, there isn't a single point at which it

begins or ends. Instead, it comes from building strategy and working to ensure that the risk-transfer mechanisms that work for more traditional threats are also brought to bear on new cyber threats.

Responsibility for cyber resilience is question of strategy rather than tactics. Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and mitigating risks. While it is everyone's responsibility to cooperate in order to ensure greater cyber resilience, leaders who set the strategy for an organization are ultimately responsible, and have increasinglybeenheldaccountable for including cyber resilience in organizational strategy [13].

The real cybersecurity challenge is the unknown. Former US Secretary of Defense Donald Rumsfeld gave the explanation of this during a news briefing in 2002: "There are known knowns. These are the things that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. These are things we don't know we don't know [14].

4.2 Cyber Threat Awareness

In a day and age when everything and everyone is connected, 24/7 and when the personal and valuable data of customers, employees and organization is accessible to anyone in the world who has the determination to gain access, digital resilience as a process and management methodology is extremely valuable. Digital resilience is all about the management of risk. The risks to data security are now so subtle, personalized and distributed that detecting threats and fully understanding these risks is becoming increasingly difficult [15].

The Internet exposes systems to cyber threats attacking information, services, and the Internet infrastructure itself. Such attacks are typically detected in a reactive fashion. The downside of this approach is that alerts of an attack are issued as it is happening.

The security community could benefit by complementing traditional reactive solutions with a proactive threat detection approach, as this would enable system to provide early warnings by analysing and detecting threat indicators in actively collected data [16].In today's information-communication environment major digital threats to many types of organizational systems are induced which calls for assessing and managing the vulnerabilities with respect to digital threats and changes.

Analysis for assessing vulnerabilities and strengths with respect to digital threats is to be performed. Then, threat scenarios that may become real are to be identified. By constructing, evaluating, and launching interventions against all identified digital threats and their critical negative outcomes, the resilience of a specific human system can be improved [17].

The evaluation of interventions is done when strengthening the adaptive capacity, i.e., a system's capability to cope with negative outcomes that may take place in the future. It is embedded in the framework of coupled human–environment systems, the theory of risk andvulnerability assessment, types of adaptation (assimilation vs. accommodation), and a comprehensive sustainability evaluation.

The number of cyber-attacks has been increased in recent years and has made cybersecurity concern for people, nations and the globe. E.g., the social media makes it possible to communicate with people who have any social media accounts. The dissemination of information through social media is fast, easy and superior to any other media. In the world, there have been approximately 2.67 billion people using social media and is expected that there will be 2.95 billion by 2020 [18].

This situation brings many problems to solve. Online attacks, terrorist activity, and cyberterrorism are most to exist. The term cyberterrorism was originated by Barry Collin in 1980 and it has spread widely and quickly to be used.

The term 'cyber terrorists' known as 'hackers' can be an individual aim to damage target's reputation. However, hackers can malign the reputations of organizations, people and even their psychological situation. The targets are generally computer networks [19].

Combating and measures may involve improving the response to cyber threats by using security technologies; developing and improving situational awareness, analytic risk mitigation scanning, adoption of international criminal law penalties and most importantly providing a holistic information security education to people and organizations that may be at risk from cyber terrorism. [20].

Within cybersecurity, threats and awareness have been categorized by United Nations Office on Drugs and Crime (UNODC) in six area as propaganda, financing, training, planning, execution and cyber-attacks [21].

The categories are explained briefly as follows:

a. Propaganda: Social media has increased the publicity of cyber terrorists by spreading their ideas with virtual tools. Terrorists try to reach out globally

to sympathizers by so-called incitement, recruitment, and radicalization. But sometimes the disseminators can be unaffiliated but are sympathetic to the ideology of a terrorist organization [22].

b. Financing: The financial resources search can comprise direct approaches, electronic commerce, virtual payment systems, and legal any financial organization. Terrorists use Web sites dedicated to the activities for summarized the money flow with secret detection methods. Social media are used to coordinate financial campaigns involve 'sponsors' and may get many amounts of cash. Terrorists can reach a large audience by peer-to-peer mobile applications such as WhatsApp and Viber or more secure ways. And sometimes donors are also a priority target group. Financing terrorist activities are done through charity organizations. Donation can be done through social media with bitcoin or with any method [23].

c. Training: Training recruits by using the Internet involves using the information to produce arms and to launch attacks. Virtual training tools are used to reach target groups and organized journals are used like Al-Qaida's Inspire. Terrorists use the Internet for collecting information about places and individuals. Recruitment is done by monitoring Facebook profiles and conversation whether they are genuine sympathizers. Terrorists add sympathizers as friends and engage in private after ensuring individuals' faithfulness. Terrorist disseminates training materials for physical attacks, and instructions to equip necessary skills for cyber defense and to improve offensive capabilities [22].

d. Planning: Existent ability of terrorists to communicate, plan, conscript, organize, and train through social media. Internet resources make it easier to plan an attack. Intelligence gathering from social media (e.g. Google earth) can be done and also they use encryption not to be discovered [24].

e. Execution: The attacks execution is hard to be detected when terrorist use right precautions when connect. The terrorists use and make chaos by targeting important infrastructures. Vulnerabilities are much and the outcomes are high. The strategies against cyberterrorism can be improved. But the threat from cyberterrorism should not be vastly overstated [25].

f. Cyber-attacks: A cyber-attack can be done at any time or place. The motivations behind the cyber-attacks are depending on the terrorist intention, hacktivism, and terrorist authorities. Organizations should take drastic protection against cyber-attacks, assess cyber readiness, expand the resilience capacity and adopts security regulations. Cyber-attacks graded from installing spyware to destroy the infrastructure. Social media attacks target websites with large user bases and use as a delivery mechanism by stealing user accounts [26].

In order to prevent and combat with cyber terrorisms, the issues summarized below should be focused and achieved.

a. Measures in social spam, campaigns, misinformation and crowdturfing, and other practical techniques should be taken into account.

b. The review showed that terrorists spread their ideas with virtual tools; have financial resources by a direct approach, e-commerce, online payment systems, and the legitimate organizations; plan, communicate, organize, recruit, and train terrorists through social media; exploit and attack by targeting critical infrastructures and vulnerabilities. These issues should be under investigation.

c. Security technologies like firewall, intrusion detection and prevention system, spam filter, anti-malware, and anti-virus tools should be used for mitigation and response of attacks.

d. Cyber terrorism measures should be preventive for information infrastructure in terms of security policy and criminal special rule's allocation. Governmental situational awareness, analytic risk mitigation scanning, and adoption of international criminal law penalties can be applied. A comprehensive education and awareness program for users and the public on cyberterrorism can contribute to decreasing cyberterrorism.

It can be concluded that combating cyber terrorisms requires more attention, knowledge, support, coordination, and experts. The managers/rulers should take actions on the issues given [20].

4.3 Digital Engagement Cyber Resilience Model

Combating known threats is an essential part of a cybersecurity strategy. It goes alongside advanced capabilities to anticipate, capture and – ultimately – learn from unknown threats. Systems have different weak spots and different processes (challenges) and they each manage risk in different ways (solutions). In other words, to each security challenge (evaluated as "known" or "unknown") corresponding solution to that challenge exists (evaluated as "knowns" or "unknowns").By incorporating values obtained during the system security assessment process into the model we get "known knowns" relating to information security, "known unknowns" relating to to cybersecurity and "unknown unknows" related to cyber resilience [27].

Example 1: There is a known crisis in the cybersecurity workforce: a massive shortfall in qualified and trained security professionals. There is also an unknown solution to this crisis. The broad and growing scope of the challenge requires a corresponding broadening of skill sets that are both known and unknown [12].

Finally, Resilience Model structure and content is presented (Figure 3), consisting of information security (Confidentiality, Integrity and Availability – CIA triad threats and responses to them i.e – known knowns), cybersecurity (non-CIA complex threats, Advanced Persistent Threats – APTs and corresponding responses to them i.e. known unknowns) and cyber resilience (unforeseeable and unpredictable threats and responses to them – unknown unknowns), the most dangerous new malware attacks, targeted rather than random, often crafted for a specific attack. In IT security industry known as Zero Day Attacks (Exploits).

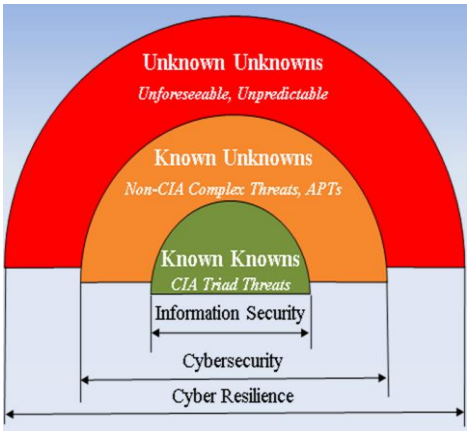


Figure 3: Digital Engagement Cyber Resilience Model

There are opportunities around those cybersecurity solutions that can take the fear factor out of unknown quantities and make them "known". But there continue to be significant opportunities around those protection measures that apply the universe of known cyber threat knowledge, to keep the system continuously secure [27].

In order to cope with the growing challenges, which today are manifested as unknown unknowns, systems tend to enable personnel and adjust existing and develop new processes, organization and technology. Technologies are being developed which, unlike traditional approaches, have the ability to protect system from serious threats by learning what is "normal" for the organization and its people and thereby spotting emerging anomalies. Unlike, the traditional rules and signature-based approach, the technology can spot threats that could harm organization and network that the traditional approaches are unable to detect. It can deal with uncertainty and delivers adaptive protection for organizations from both insider threats and advanced cyberattacks.

4.4. Strategies to Manage Risk for Digital Resilience

Example 2: Strategies for digital risk management are proposed [15]:

a. Define Acceptable Risks

Before you begin to develop any strategies to deal with data breaches and cyber-attacks, it's important that you define and understand the risks involved and set risk level based on objectives. Understanding what are and what are not acceptable risks will help you to better develop strategies to cope with incidents when they occur.

b. Develop Strategy

Once you have established a robust list of the risks to organizations data, it's time to develop high-level policies that should be used to help control, prevent and deter attacks.

c. Design Management System

Once you've developed policies and procedures to deal with potential attacks, you will need to develop a management system/process, as well as the controls needed in order to deal with incidents when they occur. This should involve delegating responsibility for cyber resilience and making sure that everyone knows what they need to do, when they need to do it.

d. Test & Transition

Having policies, management system and controls in place, you then need to thoroughly rehearse and test these procedures so that you are ready to act as soon as a threat has been detected. Once you have completed testing, you should begin to transition all elements into operational use.

e. Operation & Continual Improvement

Once in operation you should continually monitor all aspects of controls, detection methods and management procedures to ensure that cyber resilience continues to provide the level of protection organization requires in a constantly evolving environment. Remember, the pace of change is quick.

f. Communication & Discussion

Keep cyber resilience at the forefront of organizations operations and maintain discussions and communication between board members at regular meetings. It's also important to document and communicate any decisions made with regards to cyber resilience throughout the organization.

g. Maintain Balance

Constantly review controls in order to maintain the right balance between preventative, detective and corrective controls. A heavy bias towards prevention with insufficient focus on detection and correction is not a good idea. As mentioned previously, a threat that goes undetected for weeks, months or years can have a huge impact on organization.

h. Inform Employees

It's important to make sure that a balance is struck between a focus on technology controls and making sure that employees are motivated, effectively trained and periodically reminded of the importance to be ready to respond to and take seriously any threats that are detected. Investment in both security technologies and staff training will be wasted if one does not complement the other.

i. Emerging Threats

It should be a priority for those involved in cyber resilience to keep up to date with emerging threats in order to ensure that appropriate and effective controls are in place to prevent, detect and/or deal with incidents when they occur. New threats to valuable data and the security of organizations systems emerge on a daily basis, so it is vitally important that you maintain an accurate knowledge base and risk register.

j. Effective Training

Finally, the effective training of all those involved in designing, developing and maintaining cyber resilience policies and procedures is vital. Adopting established standards and best practices will help incorporate the accumulated wisdom of many other organizations and individuals in to own cyber resilience management system. Standards and best practice frameworks such as those listed below will help you gain a better understanding of how to evaluate and instate a successful and effective cyber resilience management system:

a. ISO/IEC 27001
b. ITIL
c. ISO 27005
d. Resilia.

4.5. Risks Evaluation Using Quantitative Risk Analysis

Security officers must be ready to execute different types of analysis of the risk. Qualitative risk assessment is in many situations acceptable and satisfactory. However, in order to prioritize resources for digital security the capability to numerically evaluate risks we discussed, quantitative risk analysis is vital and crucial.

Example 3 [28]:

a. Three Point Estimate – a technique that uses the optimistic, most likely, and pessimistic values to determine the best estimate.
b. Decision Tree Analysis – a diagram that shows the implications of choosing one or other alternatives.
c. Expected Monetary Value (EMV) – a method used to establish the contingency reserves for systems' digital security.
d. Monte Carlo Analysis – a technique that uses optimistic, most likely, and pessimistic estimates to determine the total digital security cost and project (maintenance and development) completion dates.
e. Sensitivity Analysis – a technique used to determine which risks have the greatest impact on systems' digital security.
f. Fault Tree Analysis (FMEA) – the analysis of a structured diagram which identifies elements that can cause system failure.

5 Conclusion

New and emerging information systems are significantly transformingorganizational systems through new business models, opportunities, products, and services. The world is hyper connected, and the organizational systems today are competing with products from everywhere. To have a digital security leading to organization all systems' resilience in place that can help them to become and remain viable and competitive is more than necessary. Digital intelligence concept encompasses personal, network and organizational cybersecurity management. Within such a concept cyber threats awareness preventive approach to minimize the effects of cyber-attacks is crucial through inserting knowledge and consequently achieving the increase of digital security and resilience level by decreasing level of "unknown unknows", moving them towards and turning them gradually into "known unknowns" and "known knowns" sequentially. In doing so reflecting on the specifics of digital threats awareness and discussing both the potential benefits and limitations of the approach and the measures and activities to be taken is essential and required to be done.

The life cycles of modern-day information-communication systems, from the process of planning, introduction and usage to their withdrawal from use are very short, which often makes their systematic testing impossible and is most commonly applied as an exception, in expressly prescribed cases. Awareness, resilience and response are at the heart of EU action to counter hybrid threats. EU is

improving the capacity to detect and understand malicious activities at an early stage. At the same time, the EU enhances the resilience of critical infrastructure, societies and institutions. This is fundamental to improving the ability to withstand and recover from attacks [29]. The cyber defense helps in improving the effectiveness of security resources and security expenses, especially in critical locations [30].

Modern environment is deeply imbued with communication and information technology. People are nowadays connected using various technologies for the transmission of text, image and sound, including the increasing Internet of Things (IoT) trend. Deviations in the proper operation of these interconnected systems or their parts are no longer merely technical difficulties; they pose a danger with a global security impact. Modern societies counter them with a range of activities and measures collectively called cybersecurity.

In our paper digital security perspectives and engagement for achieving cyber resilience in today's conditions of digital security risks are examined as well as how digital threat awareness can improve digital resilience. Within the context of cyber resilience, the novel Digital Engagement Model for Cyber Resilience in information-communication environment is presented.

Further investigations of ours are directed towards finding and enabling efficient and effective processes for agile (adaptable, aware, flexible and productive) cyber resilience of the security information system able to cope with unforeseeable and unpredictable events (unknown unknowns) in inner and outer environment of the system as a whole. Key roles related to that goal have people (actors) and their performance at all levels of system's hierarchy (digital security combined with people-centric security) within overarching concept of digital intelligence.

References:

[1] McMillan R., Proctor P. E.: Cybersecurity and Digital Risk Management:CIOs Must Engage and Prepare, G00349114, Gartner, Inc., 2018.

[2] Kim, S. D.: Characterizing unknown unknowns. Paper presented at PMI® Global Congress 2012—North America, Vancouver, British Columbia, Canada. Newtown Square, PA: Project Management Institute, 2012.

[3] Cyber Defense, available athttps://www.techopedia.com/definition/6705/cyber-defense, Accessed: 10th February 2017.

[4] Robert S. Dewar, ed.: National Cybersecurity and Cyberdefense Policy Snapshots: Collection1,Centre for Security Studies (CSS), ETH Zürich, 2018.

[5] United States: Strategy for Operating in Cyberspace, Department of Defense, 2011.

[6] Pescatore, J.: Toward a National Cybersecurity Strategy, G00167598, Gartner, Inc., 2009.

[7] NATO Cyber Cooperative Cyber Defense Center of Excellence Tallin Estonia, available athttps://ccdcoe.org/cyber-definitions.html, Accessed: 10th February 2017.

[8] Infosecurity, available at http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-gaIncreasing-Complexity4.jpg, Accessed: 15th November 2016.

[9] Marvell, S.: The real and present threat of a cyber breach demands real-time risk management, Acuity Risk Management, 2015.

[10] Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham, 2015.

[11] Hulme, G.V: Security spending continues to run a step behind the threats, available at http://www.csoonline.com/article/2134074/strategic-planning-erm/security-spending-continues-to-run-a-step-behind-the-threats.html, Accessed: 3rd June 2017.

[12] Goche, M., Gouveia, W.: Why Cyber Security Is Not Enough: You Need Cyber Resilience, available athttps://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/#562402a21bc4, Accessed: 1st June 2017.

[13] Dobrygowski, D.: Cyber resilience: everything you (really) need to know, available at http://https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/, Accessed: 21st June 2017.

[14] Tucker, E.: Official: FBI probing attempted cyber breach of NY Times, available at http://www.federaltimes.com/articles/official-fbi-probing-attempted-cyber-breach-of-ny-times, Accessed: 31st May 2017.

[15] Purple Griffon: The Importance Of Cyber Resilience (10 Strategies That Will Change The Way You Manage Risk), available at https://purplegriffon.com/blog/cyber-resilience-managing-risk, Accessed: 26th April 2020.

[16] van der Toorn, O.I., Sperotto, A.: Looking Beyond the Horizon: Thoughts on Proactive Detection of Threats. Digital Threats: Research and Practice. 2020 Mar;1(1). 4., available at https://doi.org/10.1145/3373639, Accessed: 27th April 2020.
[17] Scholz, R.W.: Digital Threat and Vulnerability Management: The SVIDT Method. Sustainability [Internet] 2017;9(4):554., available athttp://dx.doi.org/10.3390/ su9040554, Accessed: 28th April 2020.
[18] Kirichenko, L., Radivilova, T., Carlsson, A.: Detecting cyber threats through social network analysis: short survey." abs/1805.06680, 2018.
[19] Narula, S., Jindal, N.: Social Media, Indian Youth and Cyber Terrorism Awareness: A Comparative Analysis. *J Mass Communication Journalism* 5:246, 2017.
[20] Parlakkılıç, A.: Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach,*International Journal of Information Security Science*,Vol. 7, No. 4, pp.172-178., available athttp://ijiss.org/ijiss/index.php/ijiss/ article/view/349/pdf 67,Accessed: 30thJanuary 2020.
[21]United Nations Office on Drugs and Crime: The use of the internet for terrorist purposes., pp.3-13., available at https://www.unodc.org/ documents/frontpage/Use_of_Internet_for_Ter rorist_Purposes.pdf, Accessed: 10th April 2020.
[22] Shaffer, K.: 10 ways to get started fighting internet propaganda, available at https://pushpullfork.com/getting-started-fighting-internet-propaganda/, 2017, Accessed: 29th April 2020.
[23]Nazir, M.:How touse Social Media Effectively in the Media Mix, available at https://wearesocial.com/blog/2018/01/use-social-media-effectively-media-mix,2018, Accessed: 26th April 2020.
[24]Willis, H.H., Morral, A.R., Kellyand, T.K., Medby. J.: Estimating Terrorism Risk. MG-388-RC. Santa Monica, CA, RAND Corporation, 2005.
[25]Chuipka, A.: The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorists? available at https://ruor.uottawa.ca/bitstream/ 10393/35695/1/CHUIPKA%2C%20Adam%20 20169.pdf, 2017, Accessed: 20th April 2020.
[26]Sreenu, M.: A General Study on Cyber-Attacks on Social Networks, IOSR *Journal of Computer Engineering* (IOSR-JCE), Vol. 19, No. 5, 2017.
[27] Exclusive Networks:Unknown Unknowns-The Ultimate Test for Cybersecurity, available athttp://www.exclusivenetworks.com/uk/blog/unknown-unknowns-ultimate-test-cybersecurity/, Accessed: 1st June 2017.
[28] The Project Risk Management Academy: Risks Evaluation Using Quantitative Risk Analysis,available at https://projectriskcoach.com/ evaluating-risks-using-quantitative-risk-analysis, Accessed: 23rdMay2020
[29] Galinec, D., Steingartner, W., Zebić, V.: Cyber Rapid Response Team: An Option within Hybrid Threats.Proceedings15th International Scientific Conference on Informatics, Poprad,Slovakia, November 20th-22nd, 2019,
[30] Galinec, D., Možnik, D. and Guberina, B.: Cybersecurity and cyber defense: national level strategic approach, *Automatika*, Vol. 58, No. 3, pp. 266–272, 2017.