DEFENCE RESOURCE PLANNING IN THE ENVIRONMENT OF THE INTERNET OF THINGS

Nedko Tagarev*

Introduction

The *problem* of this article is the lack of defence resource planning for the moment when the conventional resources like for example weapons, will get fully in the digital age. If we want to keep up with the mainstream or the best standards in the defence practices, the planning has to start now and the defence agencies have to predict it for at least the next four decades. As the smarthouses and smartindustries are a reality, soon there will be smart cities, smart education and of course smartdefence forces. These forces include *defensive* and *offensive cyber-weapons*. These weapons often by mistake are limited to cyberspace but in reality, *Modern warfare implements* a huge range of *digital technologies* – from military robots to laser weapons. The *goal* of this article is to show the changes in Defence Resource Planning(DRP) with the implementation of the Internet of Things (IoT).

The changes in implementation of smart technologies in warfare are in process and they will be common practice in the next ten years. This process will end in the middle of the 40ties of 21 century. If we plan to have a country and military, then we cannot neglect these processes of digitalization of defence assets. In 2018, it is very hard to *predict, forecast or make prophesy* about what will be the future. In most, all of it *depends on different social factors* like *political influence, religion, cultural aspects, financial fluctuations etc*. Also, there are IT investments with steady trends that will gain their high in 2025-2040 (military sphere). Some of IT investments with defence purposes are in the prototype phase. (Tagarev, 2018) One of the main assumptions in this article is that IoT will control the objects of the *Critical Infrastructure*. For example, there are smartsociety projects in Japan. In such a situation, the goals of the potential attacker will be to destroy or put out of order the entire critical infrastructure, sector from economy, industry or region. In these cases, *the obligation of defence forces* is for response or counter-attack.

* Nedko Tagarev, Sen. Assist. Prof. PhD, Department of National and Regional Security, UNWE, email: ntagarev@e-dnrs.org

The *object* of this article is the DRP system and the *subject* is the change in the DRP system/requirements with the implementation of the IoT. The object and the subject are explained in details in Part one and Part two of this article.

The experts can measure DRP system by the requirements of the capabilities of defence forces. The measurement includes the capabilities in digital/cyber warfare, estimation of security and security threats, which are rapidly changing in the digital environment, directly connects to the DRP." Although security assessment is a specific process that requires specialized knowledge and skills to collect and process statistical information, additional data sources are used, and in many cases, executive software managers are increasingly paying attention to this process. Reasons can be seen in different directions in particular – the beneficial effects that evaluation can provide" (Цветков, 2014). In the future digital society, in the defence, Industry 4.0 and Industry 5.0 the *IoT will dominate acquisition activities*. In every common human profession, we are implementing the humanless manufacturing and services. As almost self-sufficient "organism" IoT infrastructure will *automatically implement ERP models* for planning the resources for defence.

The *scope* of the study is limited to Bulgarian processes in DRP and its defence allegiances to NATO and the EU.

The *methodology* that is used in this article includes *documentary analyses* (Bowen, 2013), *process and analogy analyses*(Bartha, 2016) and *case studies analysis*. In practice for measurement of defence, capabilities are used statistical analyses. In their essence, they measure the size of investments in different assets. The reality proofs in many examples that these analyses are not very accurate. For example, the Saudi Arabia army is one of the worlds best funded by finances and military technology, but they have a serious problem in a war with North Yemen, one of the poorest regions in the world. They do not have 21st-century military technology or finance resource close to any other military force, even that they have some support by Iran. Another example is the operation of France and Italy in Libya where on the third day, as a result of supply problems there had to be interference and support from the USA so that the operation completes successfully in favour of the France, Italy and USA. The above examples confirm that *requirements to the methodology for analyses must stay close to reality* and *common sense* and we cannot trust only statistics and account data. Therefore, the goal of planning is set on quality, non-on quantity results.

The author suggests three main *hypotheses* in this article:

- The implementation of smart technologies that communicate by IoT concept will have a major impact on military production/acquisition or everything will be "smart" and will communicate without or with minimal human interference;

- The implementation of smart technologies that communicate by IoT concept will have a medium impact on military production/acquisition or it will depend on the number of affordable resources;
- The implementation of smart technologies that communicate by IoT concept will have insignificant to no impact on military production/acquisition, the cost will be too great, or the threats will be out of control.

The paper *originality* connects to the fact that there cannot be found any publications in this area from an economic or management point of view. This approach covers the basics of the problem, but there are no previous studies related to this topic. Until now, the DRP and IoT are looked as different elements of the same system. The *goal* of the study is to combine these objects in a different approach.

This publication is for audiences who are interested in the DRP process and the introduction of new digital technologies.

The background of the article

Department of "National and Regional Security" at the University of National and World Economy is the leading scientific institution for security and defence economics in Bulgaria. The department has over 400 publications and 30 scientific projects connected partially or fully to the problem in this article.

In the teaching modules, there are disciplines that are implementing Defence Resource Management (DRM), Defence acquisition, Defence economic analyses etc. The Enterprise Resource Planning (ERP) is implemented in teaching modules in teaching course of Information technologies (Тагарев, 2018).

1. Internet of Things (IoT) environment (definition and main goal)

Based on "smart technologies" stands the IoT. "Smart technologies" concept is a constant for this article. The thing that concerns the discussed topic is the function of smart technologies. There are two main purposes for the implementation of them. The first one is to replace some human activities (week spots in human activities. Part two presents some of the weaknesses in the DRP system in Bulgaria). The second purpose is to replace a highly qualified person with some low qualified ones through implementation of smart technologies or computer technologies in general. This process can be observed not just in the digital sphere. The digital technologies allow allot of unseen before opportunities. For example the "case of taxi and Uber" (Taleb, 2018). DRP system or military products as general can apply this model of analogy.

The next decade will provide a dramatic change in the environment of security and defence. Implementation of IoT technology over all human activities define this change. Probably, The IoT is a smart approach to the problems who will provide automated solutions in a defence environment. That also concerns the DRP

systems. As a smart technology, the IoT will provide an automated implementation of ERP models that will provide a smart solution to some problems concerning planning. The human factor is often the reason for these problems. Also, this automated approach IoT will eliminate many problems concerning facilitation of the critical infrastructure in Bulgaria as in the other parts of the world.

IoT Definition [1]
The internet of things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The method of communication is closely identified with RFID (Radio-frequency identification), although it also may include other sensor technologies, wireless technologies or QR codes (quick response code).

The IoT is significant because an object that can represent itself digitally becomes something greater than the object by itself. Surrounding objects and database data connects to the object, which is related not just to its user. When many objects act in unison, they had "ambient intelligence."

The IoT is the most commonly used term and aspect of the digital future. There is another concept that can explain processes in the military and defence sector – the Web of Things (WoT).

WoT Definition
The Web of Things (WoT) is a computing concept that describes a future where everyday objects are fully integrated with the Web. The prerequisite for WoT is for the "things" to have embedded computer systems that enable communication with the Web. Such smart devices would then be able to communicate with each other using existing Web standards.[2]

This definition presents a connection between all military/defence capabilities by themselves excluding human intervention. In 1998, this concept was a sci-fi approach. In 2018, it is a near future reality. The IoT changes the scope of DRP in a huge way as it changes the object and range of operation of defence forces. For example, Chinese military doctrine that aimed at "inflicting a heavy toll on the enemy, even the conventionally superior one, through a variety of tools ranging from the destruction of its satellites and missile systems to the use of electromagnetic pulse weapons to hit enemy ships or aircraft and even its civilian IT networks" [3]. That also changes the border of operation as they are not limited

to the physical border of the state of China as they expand to all of the cyber actives of the country[4].

For example, of the human mistake that can be eliminated is a case when a Belgian Air Component F-16 fighter was destroyed and a second plane severely damaged after two maintainers accidentally triggered another jet's Gatling gun. Two other Belgian Air Force personnel on the ground were treated for injuries (Mizokami, 2018). IoT can easily eliminate such kind of problems, by the smart technologies that communicate between themselves.

There are thousands of examples of implementation of smart technologies in military units even without technical approach. "From ongoing production today through testing and full service in the future, the F-35 will seamlessly incorporate the latest technological advancements as they emerge. It has specifically developed a solid aerodynamic design is with room to grow, a room that will continue to ensure that the F-35 will be a highly adaptable platform ready to accommodate rapidly changing technologies. The F-35 is a smart fighter that will get even smarter as new threats and the technologies to counter them emerge"[5]. Smart weapons show such an approach for more than twenty years. Two examples show that – "The first weapon is the Lockheed Martin-produced Wind-Corrected Munitions Dispenser (WCMD), which features an inertial reference system that corrects for actual wind effects during the bomb's fall. From high altitude, delivering of the weapon is accurate. The cluster weapon comes in three versions, depending on submunition, i. e., CBU-103 (BLU-97 combined effects munitions), CBU-104 (BLU-91/92 mines) and CBU-105 (BLU-108 anti-armor sensor-fused weapons)" (Dewitte, 2000) and "The other new smart weapon, the EGBU-27 guided bomb, has an improved 2,000-pound 'bunker buster' warhead and multisensory guidance. This weapon can be used either as a precision laser-guided bomb or, if the target coordinates are known, it can use its GPS/INS sensor for guidance as a near-precision, all-weather, 'launch-and-leave' weapon" (Dewitte, 2000).

The main goal of implementation of smart technologies is simple – to replace the human factor in future warfare, and the IoT and/or WoT technologies. This allows the smart devices to communicate between themselves and replace humans. There are two main reasons for replacing humans – the social one and the economic one. Human casualties in military activities are a connection to the social aspects. In addition, humans make intentional and unintentional mistakes. The economical one is the cost of education for military personnel. According to the DoD of the USA in 1999, the cost to train each military pilot through basic flight training is about $1 million and the cost to fully train a pilot with the requisite operational experience can be more than $9 million [6]. The other support for these conclusions can also be found in the UK Ministry of Defence "Improvement Plan"[7].

2. DRP system in Bulgaria

The Bulgarian practice in DRP is connected to Planning Programming Budgeting System(PPBS) (DonVito, 1961) under the Law on Defence and Armed Forces of the Republic of Bulgaria[8].

PPBS is an integrated management system that places emphasis on the use of analysis for program decision making. It is a standard in the US from the 90-ties. The purpose of PPBS is to provide management with a better analytical basis for making program decisions, and for putting such decisions into operation through an integration of the planning, programming and budget functions. Program decision making is a fundamental function of management. It involves making basic choices as to the direction of an organization's effort and allocating resources accordingly. This function consists first of defining the objectives of the organization, then deciding on the measures that will be taken in pursuit of those goals, and finally putting the selected courses of action into effect[9].

The PPBS is an output-oriented model. PPBS places major emphasis on the identification of program objectives and the measurement of "results" or "output" in quantitative terms. However, identification of "output" or "results' '-oriented objectives is very difficult in the natural resources area. In fact, the problem at present in implementing PPBS in the natural-resource oriented agencies is finding the output-oriented program categories to implement the system (Hooper, 1968).

The way to evaluate the system by the analogy methodology is to implement System Maturity Evaluation[10]. Table 1 shows the model.

Table 1. System maturity model – evaluation

Level of Maturity	The maturity of the System	Management of the processes
0	**Non-existent**	*Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.*
1	**Initial/Ad Hoc**	*There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.*

2	**Repeatable but Intuitive**	*Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.*
3	**Defined**	*Procedures have been standardised and documented and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.*
4	**Managed and Measurable**	*Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.*
5	**Optimised**	*Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.*

3. Defence resource planning and Enterprise resource planning. *Where are the differences?*

Defence resource planning

Defence resource planning (DRP) is part of the Defence Resource Management (DRM) that provides the government with "a realistic perspective on the benefits of and obstacles to adopting comprehensive processes for managing defence resources, and provide an organized context for thinking about the ongoing evolution of established systems." (Gordon and Hinkle, 2011). *DRM is a national obligation*. To reach the goal *there have to be achievable defence objects* that are

realistic for national capabilities as there has to be applied *independent analyses*. DRM includes four steps in planning as Fig 1 shows the process.

- Strategic planning;
- Capability planning;
- Resource planning;
- Acquisition planning.

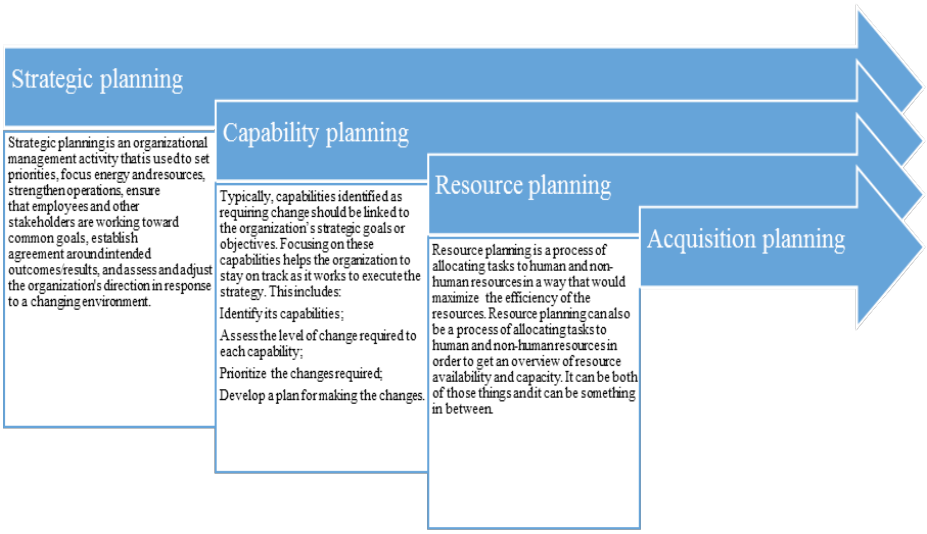

Fig. 1. The sequence of the DRM process

By military assets, we are measuring and evaluating defence capabilities. These abilities are defined as a set of resources, the combination of which makes it possible to perform tasks in specific conditions and in a manner that meets a certain standard (Георгиев, 2014). Plan-Do-Check-Act (PDCA) model manage this process. Fig. 2. represents this process analysis.

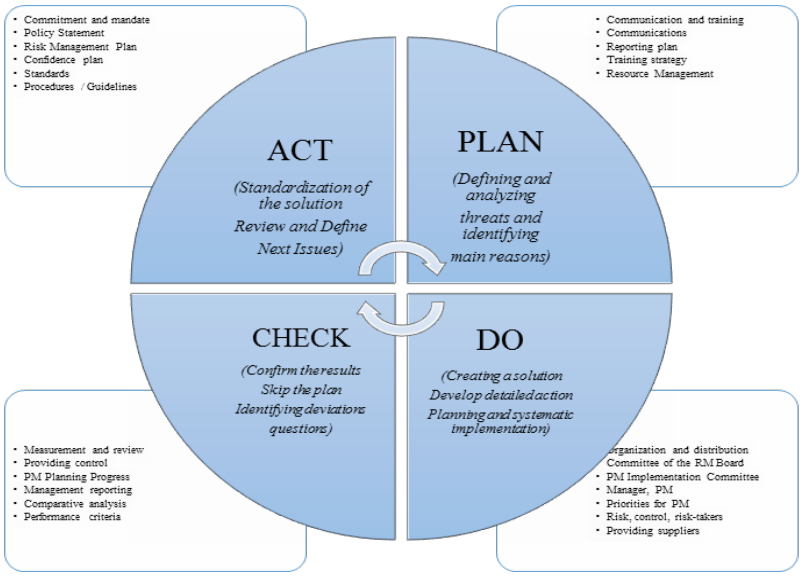

Fig. 2. PDCA model

DRP is one of the most important government's obligation everywhere in the world. It includes a huge amount of financial resources, material ones, and people, movable and immovable property. "The modern development of the armed forces implies the effective implementation of democratic control. Democratic control goes far beyond the scope of "civilian-military relations." It imposes both civilian control of the Armed Forces in the exercise of the right of civilians to control the military, as well as the active engagement of the whole society in this process" (Пудин, 2009). Implementation of digital technologies facilitates more and more control of this process. Therefore, the policy and policy-making process have to be very *careful* and *responsible* for spending and distributing such amount of money. The problems concerning DRP connects directly with decision-making. According to future threats, the decisions authorities made are at the environment of big uncertainty for the future. Defence capabilities that will be needed, in the digital era, are hard to predict. Often the approach to face an environment of uncertainty is Robust Decision Making (RDM). RDM rests on a simple concept. Rather than using models, data, and constraining options to describe a best-estimate future, RDM runs models using hundreds, thousands, or even millions of different sets of assumptions to describe how plans perform in many possible future variants/scenarios for the future. The approach then based on using statistics and visualizations resulting in a large database of model runs to help decision makers to identify those future conditions where their plans will

perform well or will fail. This information can help decision-makers to develop plans that are more robust to a wide range of future conditions.(Lempert et al., 2016) In addition, for example, RDM "is an iterative, quantitative, decision support methodology designed to address the challenges of predictive failure. The approach has been applied to areas outside national security, such as flood risk." (Fischbach, 2010) In the IoT system, the Big data analyses will provide automatic "Risk management process"[11]. ERP automated this process.

A good example of a not well-performed policy, resource planning and acquisition process is the acquisition of new fighter jet intended for the Bulgarian air force. That process continues twenty years and actually becomes in the past year a real political problem. The background of these problems comes from the ending resources of the current fighter jets. The other is the defence obligation of Bulgaria to NATO and EU including "Air Policing" *(The use of interceptor aircraft, in peacetime, for the purpose of preserving the integrity of specified airspace*[12]*)* which "is the only military mission on the territory of Bulgaria. However, our country is not alone in air defence missions on the Balkans and NATO allies"[13]. There are also history, tradition and social elements that concerns Bulgarian military air force. Probably until the end of this process of acquisition, these new planes will be unusable because of mass usage of *humanless automated technologies*. This period does not include the 2-3 year period of delivery of aircraft and training the personal – pilots and land support personnel. This connects to the future mass implementation of digital technologies in the defence sphere. The problems that are seen and are the main reasons for the delay of this project are common with the problems that can be observed in other projects or programs in Bulgarian defence policy:

- Lack of resources- financial, human, infrastructure and so on;
- Lack and/or bad planning;
- Illiteracy, incompetence or corruption (there are no evidence for those);
- Alternatively, a combination of all of those.
- Weaknesses of the human factor provoke these problems. Probably there have to be considered some other *alternative solutions*. In some cases, they are more cost-effective than this acquisition of aircraft:
- Take actives by rent;
- Public-private partnership;
- Hire a private mercenary army;
- Hire other military force;
- *Acquisition or development of humanless aircraft*;
- Etc.

So probably, the best solution for Bulgaria is not a reactive but proactive approach. As the examples show, the limited resources have to be concentrated on

the *future digital technologies instead of conventional ones.* In the environment of IoT, this will *give the Bulgarian military overtaking threats capabilities*.

The importance of financial resource

According to the resources in Bulgaria "the reduction of the defence budget over the years from 2.5% of GDP to 1.2-1.3% of GDP cannot be classified in any other way except drastically and significantly. The defence budget is both a percentage of GDP and an absolute amount. In real terms, if the impact of inflation is removed, the surplus is even higher" (Д. Димитров, 2014).

For planning and allocation of the resources, there is a Directorate in the Ministry of Defence that has functions and duties[14] including *Organizing the Defence Resource Management Integrated System within the Ministry of Defence, the structures directly subordinated to the Minister of Defence, and within the Bulgarian Armed Forces*.

"The rule" of profit/revenue for DRP

There is a big difference between Defence resource planning (DRP) and Enterprise resource planning ("business" planning). Often the major problem concerning limitation of resources is that the investment in military/defence actives has no revenue. In the enterprise/business, projects the goal is revenue even that the process in both objects is the same. The military industrial complex is an exception of this rule of profit/revenue that is specific for the resource planning of defence. "Military-industrial complex is a network of individuals and institutions involved in the production of weapons and military technologies. The military-industrial complex in a country typically attempts to marshal political support for continued or increased military spending by the national government."[15] U.S. President Dwight D. Eisenhower in his Farewell Address first used the term military-industrial complex on January 17, 1961. Eisenhower warned that the United States must "guard against the acquisition of unwarranted influence by the military-industrial complex," which included members of Congress from districts dependent on military industries, the Department of Defence (along with the military services), and privately owned military contractors (e.g., Boeing, Lockheed Martin, and Northrop Grumman). Eisenhower believed that the military-industrial complex tended to promote policies that might not be in the country's best interest (such as participation in the nuclear arms race), and he feared that its growing influence if left unchecked, could undermine American democracy.(Eisenhower, 1961) There have to be mentioned that there are a variety of different national policies in this direction that directly influence the DRP, and the "evolution of the relationship between scientific research, industry and national defence" (Else, 2017). For example in the USA there was a transition shifted from publicly owned companies to private firms during the first half of

the 20th century (Publication, 2005). In 2018 this approach is a reality with the proposed investments in 2019 budget included Lockheed Martin's overpriced, underperforming F-35 aircraft, at $10.6 billion. Boeing's F-18 "Super Hornet," which was in the process of being phased out by the Obama administration but is now written in for $2.4 billion. Northrop Grumman's B-21 nuclear bomber at $2.3 billion; General Dynamics' Ohio-class ballistic missile submarine at $3.9 billion. $12 billion for an array of missile-defense programs that will redound to the benefit of Lockheed Martin, Raytheon, and Boeing, among other companies (Hartung, 2018). In France, the national government still own and manage most of the military-related enterprises. In EU ownership has an international scope, producing weapons systems like Eurofighter [16] that involve the military firms of several different countries. Countries bases these practices on the market-orientation. This direct concern DRP.

Experts compare expenses in DRP to benefits. In the military, we cannot measure benefits by profit values. In most cases, defence resources are used only for military purposes. The main methodology about the evaluation of the effectiveness and efficiency of military/defence investments is "cost-benefit" analyses. Also, some policies and international determine the expenditures. Also, there is a social role for military/defence expenditures. There are other connected activities like maintaining infrastructure, education, and healthcare and so on. The military/defence forces and investments are key factors for the development of different country regions, but "The careful reading of the National Strategy for Regional Development of the Republic of Bulgaria for the period 2012-2022 from 2012 instead of creating hopes and confidence of the national development policy revives the internal and interregional differences and disproportions" (Иванов, 2014).

There is a prognostic assumption, with good chances for happening is the steady increase in Information Technologies (IT) for military purposes. In Chart 1. "Military spends per year trends" are shown the total amount of military expenditure trends in the world. Also, have to be mentioned that there are no full data for all the countries in the world. (Tagarev, 2018) The data[17] is taken from the SIPRI Military Expenditure Database [18].

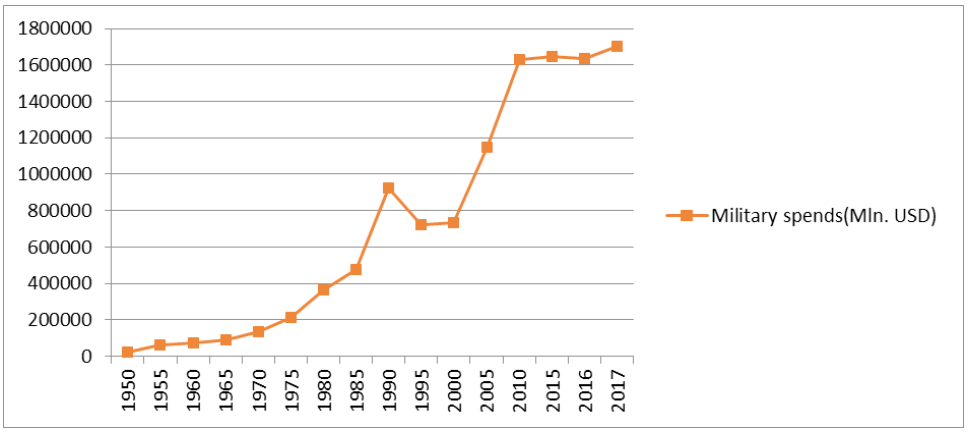

Chart 1. "Military spends per year trends"

USA policy is a good standard for planning and management of defence resources. There has to be noticed that in every different sector there is independent research and manufacturing of military digital technologies that are connected in a cyber-network. The private sector is connected to some independent cyber technologies. Also, we can compare the structure of expenditures. In Table 1. can be seen Spends the budget of the US in 2017 and Bulgaria 2018. There have to be clear that this comparison is just to find a pattern for expenses.

Table 2. Spends the budget of the US in 2017 and Bulgaria 2018

Total Budget	**FY 2017 Request US/ USD**(Norquist, 2017)	**In %**	**FY 2018 BG/ BGN**	**In %**
Military Personnel	138831498	24%	911 730	76%
Operation and Maintenance	250894310	43%	55 364	5%
Procurement	112081088	19%		0%
RDT&E	71765940	12%	2 528	0%*
Revolving and Management Funds	1512246	0%*	2 528	0%*
Military Construction	6296653	1%		0%
Family Housing	1319852	0%*	1 020	0%*
Total	**582701587**	100%	**1 193 319**	100%
* – under 1 %				

There can be seen clear asymmetry in expenditures when we compare it in relative value. In Chart 2. is visualized the different symmetry in budget spends. In this asymmetry in spendings, we can see clearly the effect of economic and political factors. These types of budget spending will affect defence capabilities in the digital future. "Economic factors that have a direct impact on arms development projects are related to the wealth of the state expressed in GDP and the decision on how much of it to be allocated for defence." (Ценков, 2014)

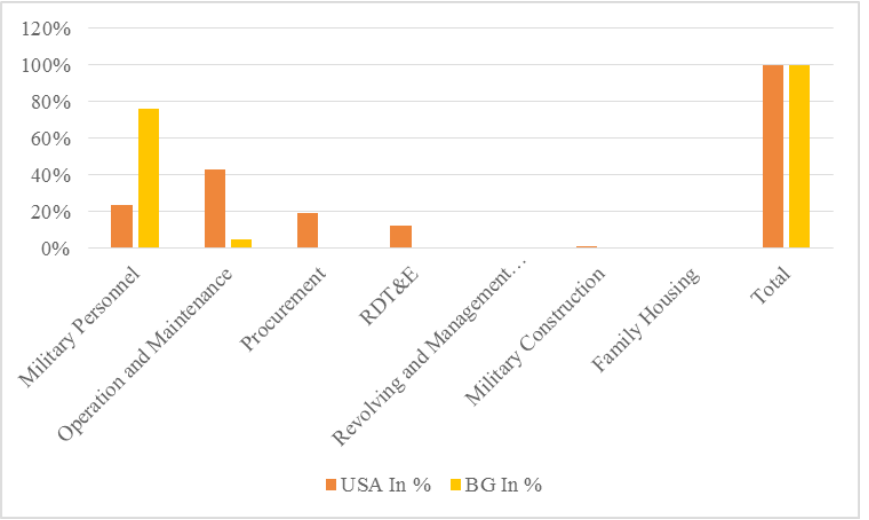

Chart 2. Asymmetry in budget spends in two studied countries

In Bulgaria, another factor limits the financial resources for defence acquisition. In the acquisition process, the Bulgarian Ministry of Defence has to pay VAT and Import duties.

The positions in the budget in Bulgaria and the US are different. They can be compared in some of the basic positions. In Bulgarian defence budget have to be noted following type of expenditures for 2018 – total 1 193 319. Staff – 911 730.0; Subsidies and other current transfers 2 528; Subsidies and other current transfers to non-financial corporation's 2 528.0; Current transfers, benefits and benefits to households 1 020.0; Capital costs 55 364; Acquisition of fixed assets and overhaul 55 364[19].

Forecasting the future for the year 2019 in the US the priorities will be – Mission support activities: $66.8 billion, Aircraft and related systems: $55.2 billion, Shipbuilding and maritime systems: $33.1 billion, Missiles and munitions: $20.7 billion, Ground systems: $15.9 billion, Science and Technology $13.7 billion, Missile defence programs: $12 billion, C4I systems: $10 billion,

Space-based systems: $9.3 billion.(Mehta, 2017) In each of these priority lines, there is a particular budget for IT investments. This is linked with "Shaping the Army Network:2025-2040" which explain required capability areas and the IT technologies including dynamic transport, computing and edge sensors; data to decisive action; human cognitive enhancement; robotics and autonomous operations; cybersecurity and resiliency.[20]

When we implement the digital society in DRP there have to be integrated some cyber solution to the planning. Such solutions are ERP models.

Enterprise resource planning (ERP)

ERP models are the most recognizable approach for implementation of innovation and investments from *planning to realization*. If Bulgarian defence policy "decide" to go to the 21st century, the ERP is probably the best approach and automated connection to the IoT.

Implementation of digital technologies on a mass scale requires a lot of innovations and investments. In this implementation, we need to keep in mind that "first of all, the investment cannot be considered as separate acts or events, isolated from their predecessors and subsequent events. Making innovation is the result of a prolonged process of resource transformation and progress – scientific, technological, technical, and so on. The outcome of an investment depends to a large extent on the characteristics of the previous investments and at the same time creates conditions for the beneficial effect of further investments".(Цветков, 2004)

Bulgaria has experience in implementing and usage of digital instruments in digital defence process. For example, Bulgarian armed forces participate in joint training in Lock Shields (LS14), a network security exercise together with 17 other countries(Тагарев, 2014a). Another example is the Automated Information System in the Ministry of Defence – "that includes – information-accounting, technological, and information protection"(Павлов, 2003).

Enterprise resource planning (ERP) is the integrated management of business processes, finance and manufacturing[21], often in real-time and mediated by software and technology. ERP is usually referred to as a category of business-management software — typically a suite of integrated applications—that an organization can use to collect, store, manage and interpret data from these many business activities(Perkins, 2018). One of the benefits of ERP is the implementation of best practices(van Groenendaal, 2008), that allows a competitive approach for solving a problem in an uncertain environment.

Implementing ERP typically requires changes in existing business processes. (Gupta, 2011) These models have to be adapted. For the public sector, there is

Government resource planning (GRP), which is the equivalent of an ERP and an integrated office automation system for government bodies.(Yunliang et al., 2010)

The ERP covers a big amount of functions including[22] (Carnes, 2014) [23]:

- Finance & Accounting: General Ledger, Fixed Assets, payables including vouchering, matching and payment, receivables Cash Management and collections, cash management, Financial Consolidation
- Management Accounting: Budgeting, Costing, cost management, activity-based costing
- Human resources: Recruiting, training, rostering, payroll, benefits, retirement and pension plans, diversity management, retirement, separation
- Manufacturing: Engineering, bill of materials, work orders, scheduling, capacity, workflow management, quality control, manufacturing process, manufacturing projects, manufacturing flow, product lifecycle management
- Order Processing: Order to cash, order entry, credit checking, pricing, available to promise, inventory, shipping, sales analysis and reporting, sales commissioning.
- Supply chain management: Supply chain planning, supplier scheduling, product configurator, order to cash, purchasing, inventory, claim processing, and warehousing (receiving, put away, picking and packing).
- Project management: Project planning, resource planning, project costing, work breakdown structure, billing, time and expense, performance units, activity management
- Customer relationship management: Sales and marketing, commissions, service, customer contact, call centre support — CRM systems are not always considered part of ERP systems but rather Business Support systems (BSS).
- Data services: Various "self–service" interfaces for customers, suppliers and/or employees

There are some weaknesses in ERP models and software. Often the ERP propose the cheapest solution that can cover the minimal requirements. In the DRP, this disadvantage can be a benefit because of the spending of public resources, which for example are extremely limited in Bulgaria. Also, this automated model will eliminate some of the problems in planning such as incompetence or corruption.

The difference between DRP and ERP

Table 3. shows systemized differences between DRP and ERP. Several categories classify the differences – Type of organization, Resources, Places (location of operation), Methods/modes of action, Tools and Motives.

Table 3. The difference between DRP and ERP

	DRP	ERP
Type of organization	National public	National/Private
Resources	People/Polices/Strategies/ Production	People/Polices/Strategies/ Production
Places, location of operation	National/International*	National/International
Methods/modes of action	Defence and offence military capabilities	Production of product or services
Tools	Military gear	Marketing/Sales/Import/ Export/Advertisement
Goals	Protection of state independence of the foreign threats	Profit/Revenue
Motives	Defend the country	Get profit
*Export and import of special production		

By this classification, we can also analyze the military budget structure and its symmetry. Policymaking, strategies and decision-making have to be approached as an influence, even that the monetary capabilities are the most important factor in DRP. In the first place, there are social factors that include the executive and legislative power, and social opinion and expectation. In the second place, there is a membership in the military organization. In Bulgarian case, these military organizations are the NATO and EU(in some cases). On the third place, there is defence industry, export and import companies with socialization in products with dual use. In addition, other factors are often forgotten like political, economic, cultural influence of the country in the international stage. So all these factors make Bulgarian policy to have *NATO centric model of planning*. "The aim of the NATO Defence Planning Process (NDPP) is to provide a framework within, which national and Alliance defence planning activities can be harmonized to enable Allies to provide the required forces and capabilities in the most effective way. It should facilitate the timely identification, development and delivery of the necessary range of forces that are interoperable and adequately prepared, equipped, trained and supported, as well as the associated military and non-military capabilities, to undertake the Alliance's full spectrum of missions."[23].

NATO divided this process into five steps:

- Step one – Establish political guidance;

- Step two – Determine requirements;
- Step three – Apportion requirements and set targets;
- Step four – Facilitate implementation;
- Step five – Review results.

In Bulgaria, the planning is in short and medium term (up to 20 years). Probably the correct standard is to go with the USA-centric approach, where the planning is in long-term (50+ years). The planning depends on the pre-planning data, goals and activities. There are many differences in the pre-planning process when we compare Bulgaria and USA. Table 4. shows the observed differences.

Table 4. The comparison between USA/Bulgaria pre-planning

	Bulgaria	USA
Type of defence forces	National	National/Private contractors
Resources	1.2 bln. BGN per year	Over 580 bln. USD per year
Places, location of operation	National/International	National/International
Methods / modes of action	Defence	Offence/Defence
Tools	Army/Navy/Air force	Army/Navy/Air force/Nuclear force/ Cyber force/ Space force
Goals	Defend the national borders of the country	Defend the national borders of the country/ Wage war/ "World policing"
Motives	National oriented	National oriented/Market oriented

Planning of the capabilities

According/reactive to the threats we build the defence capabilities. The threats in digital society change the scope and intensity from conventional military operation to cybersecurity. These threats are directly connected to the evolution of cyber criminals and cybercriminal activities which in the 21st century are professional profit operation(Тагарев, 2014b). These threats come from individuals, groups, organizations or countries. All of them have common resources, knowledge of attack, motivation and place(Tagarev, 2015). *We classify them also as the assets of the attacker.* In the digital age, the limitation of location no longer exists. This will be in no matter at all in the age IoT. In the situation of the lack of resources, the response to the threats has to be asymmetric.

Table 5 shows the comparison in the Matrix of resource planning for capabilities against conventional threats. These threats include military threats such as foreign invasion, terrorism etc. Defence agencies construct DRP on the evaluation of these threats.

Table 5. The matrix of resource planning for capabilities against the conventional threat

Actives	Threat	Defence capabilities
Source of threat	Individuals/Groups/ Countries	Country
Resources	Finances/Technologies	Finances/ National defence system
Knowledge	Week points of defence	PPPS
Location	Physical borders of the state	Physical borders of the state
Motives	Political, Religious, Financial	Protection of the independence of the state
Goals	fear, control, domination over resources	National protection

For visualization of the change, with implementation of IoT, the author created a simplified model that can observe the shift through the process analyses. Fig. 2 shows this model. Tables also present this change for better visualization.

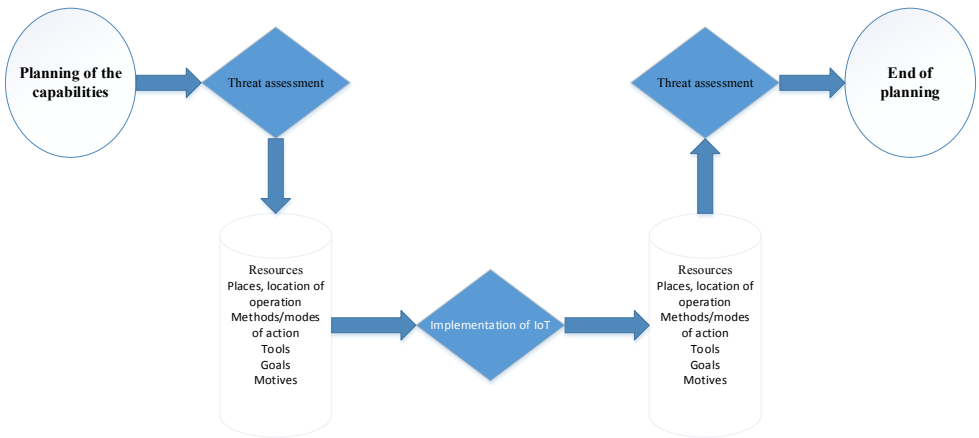

Fig. 2. Simplified process with the implementation of IoT

There is an alteration if we put the budget planning. In the environment of IoT, this is even more visible. Table 6. presents the matrix of resource planning for capabilities including IoT.

Table 6. The matrix of comparison between USA/Bulgaria including IoT

Actives	Bulgaria	USA
Type of defence forces	National/*National Cyberspace*	National/Private contractors/ *Cyberspace*
Resources	1,2 bln. BGN per year/*Electricity power independence**	Over 580 bln. USD per year/ *Electricity power*
Places, location of operation	National/International	National/International
Methods/modes of action	Defence/*Defence cyber technologies*	Offence/Defence/ *Offence and defence cyber technologies including military robots, laser weapons, automated response systems***
Tools	Army/Navy/Air force/*Cyber force*	Army/Navy/Air force/ Nuclear force/Cyber force/ Space force/ *Automated cyber force*
Goals	Defend the national borders of the country/ *Defend the cyberspace of the country****	Defend the national borders of the country/ Wage war/ "World policing"/ *Defend the cyberspace of the country*
Motives	National oriented	National oriented/Market oriented

* Electricity power is the main resource for digital technologies. The lack of electricity will lead to the stop of the existence of cyberspace. For Bulgaria as a member of EU "the energy sector of our economy is linked to the common energy policy of the EU countries and supports the realization of the strategic perspectives for the construction of the necessary infrastructure and the diversification of the energy supply"(Н. Димитров, 2014). In this stage of human technologies, the best solution seems nuclear power plants. For example, Gerald R Ford Class (CVN 78/79) – US Navy CVN 21 Carrier[25] has two A1B(700 MW) nuclear reactors.
** These weapon systems are a reality in the US military force. Their long-term plan is a total replacement of humans with machines/cyber technologies until 2040.
*** For Bulgaria, the cyberspace probably will be limited to the physical borders of the country. This is according to the factors of political and economic influence on the international stage.

The major problem for Bulgaria is the symmetry of the budget where the biggest part is military expenditures for personal. If the smart technologies and

IoT are widely embedded, there we can expect huge social tensions. *IoT and smart technologies concept excludes human labour*.

In the digital environment, the threats have an asymmetric approach. Therefore, the response has to be too asymmetric. Table 7. present the Matrix of resource planning for capabilities against conventional threat including the new cyber threads in the IoT environment.

Table 7. The matrix of resource planning for capabilities against conventional threats including the cyber treads in the IoT environment

	Threat	**Defence capabilities**
Source of threat	Individuals/Groups/ Countries	Country/*Automated Cyber Response Systems*
Resources	Finances/Technologies/*Information technologies*	Finances/ National defence system/ *Cyber defence force*
Knowledge	Week points of defence/*Cyberweapons*	PPPS/*ERP*
Location	Physical borders of the state/ *Cyberspace of the state*	Physical borders of the state/ *Cyberspace of the state*
Motives	Political, Religious, Financial	Protection of the independence of the state/ *Protection of the cyberspace of the state*
Goals	fear, control, domination over resources	National protection/ *Protection of national cyberspace*

The IoT environment generates major change in the requirements for defence capabilities. Some main changes concern the automated processes in DRP and automated reactive approach to the threats. In these analyses, we exclude the current cyberdefence capabilities so we can include smart and self-support technologies.

Conclusion

The problem discussed in this article soon will be a common problem for all the countries. This problem provides a new threat of different asymmetric approach and different scope. The third part shows the IoT change in the environment of DRP. The second part, explain the processes in DRP for Bulgaria. Author

compares the DRP in Bulgaria with these processes in the USA. For standard is used DRP process in the USA.

Author of this article makes several conclusions:

- The model of the military sphere can implement the model of the analogy of usage of smart technologies from the civil/business/social sphere. In DRP/ military activities the man's knowing/skill can be replaced if in business, for example, by smart technology it can be done.
- As the short-term goal for "smart technologies" is to replace the human activities (mistakes in human activities) there will be some implementation in the DRP system and military technologies at all.
- As the long-term goal is to replace fully humans in military activities. The IoT allow the smart technologies to communicate/share/analyze information between themselves.
- One of the reasons that the smart technologies and the IoT will define the future of military acquisition is the size of possible income for the companies that provide such solutions.
- The way to evaluate in quality measures the DRP system is by System Maturity Model. It allows comparing the policies and processes.
- There is a straight sequel in the implementation of some technology in the military sector as its public issue. The sequel is Strategic planning, Capability planning, Resource planning, Acquisition planning. This sequel cannot be changed or disturbed in the long term.
- PDCA model provides enough management practices for implementation of the IoT in DRP.
- We can base The Robust decision-making on a "big data" that is collected by IoT technology. RDM will base on the "computer decisions", in future.
- The RDM is an automated process in ERP.
- The ERP provides independence from political/social factors on which the DRP is dependent. Probably, in the case of Bulgarian bad practices and experience, there have to be tried a different approach.
- The ERP through IoT data can provide alternative solutions to the problems.
- Most of the DRP projects in Bulgaria will be useful in the time of their realization if the prediction for implementation of smart technologies and IoT are realized in the next ten years.
- There is a rule for DRP that is a non-profit activity. This is not quite right if it concerned a private/enterprise sector (the US example).
- The DRP process is directly dependent on the number of financial resources. This quantity allows the development/testing/implementation of the new technologies. According to the official data, the only country that

can freely "experiment" in the military sphere is the USA. DRP plans for 2040 represented this.

- Bulgarian DRP policy has a NATO-centric model of planning. In this state of national security policy, this is not a discussable issue. In some cases can be observed even an US-centric model of planning
- Defence agencies build their capabilities according/reactive to the threats.
- In the case of implementation of smart technologies and their communication through IoT/WoT, there have to be changed in the DRP system as the capability planning is reactive to the threats.

Conclusion according to the hypothesis:

The author opinion is that there we can make conclusions only on the first hypothesis. There will be a major impact on the DRP process with the implementation of IoT. We can assume that it will be bigger for countries/states that are users/consumers of USA military technologies, or in other word US-centric DRP approach states.

For the other hypotheses, there are not enough data or it is too early for studying the "minority effect". We have to make more detailed and broad research for minor or medium effects.

Also by lack of implementation of IoT in DRP, we can predict several problems in the future:

- A reactive not proactive approach to DRP systems;
- Serious lack of resources for defence in case of Bulgaria;
- A huge asymmetry in spending's in Bulgaria;
- The IoT and its excluding of the human factor will lead to huge social tensions;
- The structure of the threats will not change but the capabilities will, according to the future digital environment.

Notes:

[1] Techopedia, 2018 What is the Internet of Things (IoT)? – Definition from Techopedia [WWW Document]. Techopedia.com. URL https://www.techopedia.com/definition/28247/internet-of-things-iot (accessed 10.14.18).

[2] Technopedia, (2018), What is the Web of Things (WoT)? – Definition from Techopedia [WWW Document]. Techopedia.com. URL https://www.techopedia.com/definition/26834/web-of-things-wot (accessed 10.14.18).

[3] State Council Information Office China, 2004 White Paper on China's National Defense in 2004 [WWW Document]. URL https://fas.org/nuke/guide/china/doctrine/natdef2004.html (accessed 10.14.18).

[4] Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) [WWW Document], 2017. New Am. URL https://www.newamerica.org/cyberse-

curity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (accessed 10.14.18).
[5] F-35 Lightning II http://www.jsf.mil, 2018, JSF.mil > F-35 > Background [WWW Document]. URL http://www.jsf.mil/f35/f35_background.htm (accessed 1.5.19).
[6] United States General Accounting Office, 1999. MILITARY PERSONNEL/ Actions Needed to Better Define Pilot Requirements and Promote Retention (No. GAO/NSIAD-99-211).
[7] MoD UK, (2014). Ministry of Defence Improvement Plan 33.
[8] Sg, P., No. 38/18.05.2012 Law on Defence and Armed Forces of the Republic of Bulgaria 87.
[9] PGC, 2018. Planning Programming Budgeting System (PPBS). Ready Think.
[10] Information Systems Audit and Control Association (Ed.), (2012). COBIT 5: a business framework for the governance and management of enterprise IT: an ISACA® framework. ISACA, Rolling Meadows, Ill.
[11] ISO, 2009. ISO 31000 Risk management [WWW Document]. URL https://www.iso.org/iso-31000-risk-management.html (accessed 10.15.18).
[12] Air policing – definition of air policing by The Free Dictionary [WWW Document]. URL https://www.thefreedictionary.com/air+policing (accessed 10.15.18).
[13] Информационен център на МО,2014 От първо лице за Air Policing | Информационен център на Министерство на отбраната.
(lnformation center of Ministry of Defence, 2014)
[14] Ministry of Defence of the Republic of Bulgaria, (2018) Ministry of Defence of the Republic of Bulgaria [WWW Document]. URL https://www.mod.bg/en/ministry_sa_ppb.html (accessed 10.14.18).
[15] Weber, R., Military-industrial complex | Britannica.com [WWW Document]. URL https://www.britannica.com/topic/military-industrial-complex (accessed 10.14.18).
[16] eurofighter.com, 2018 Eurofighter Typhoon | The world's most advanced combat aircraft [WWW Document]. URL https://www.eurofighter.com/ (accessed 10.14.18).
[17] SIPRI, (2018). SIPRI Military Expenditure Database | SIPRI [WWW Document]. URL https://www.sipri.org/databases/milex (accessed 10.14.18b).
[18] SIPRI, 2018. "Military expenditure by country, in constant (2016) US$," SIPRI 2018. Data for all countries from 1988–2017 in constant (2016) USD [WWW Document]. URL https://www.sipri.org/sites/default/files/1_Data%20for%20all%20countries%20from%201988%E2%80%932017%20in%20constant%20%282016%29%20USD.pdf (accessed 10.14.18a).

[19] Народно Събрание на РБ of RB, 2018 ЗАКОН ЗА ДЪРЖАВНИЯ БЮДЖЕТ НА РЕПУБЛИКА БЪЛГАРИЯ ЗА 2019 Г.. URL https://www.tita.bg/laws/318 (accessed 10.14.18).
(Parlament of RB, Zakon za durjavniya budzhet na Republika Bulgaria za 2019 [WWW Document])
[20] CIO-G6, (2016). STAND-TO! [WWW Document]. www.army.mil. URL http://www.army.mil/standto/archive_2016-04-11 (accessed 10.14.18).
[21] Oracle, (2018). What is ERP System? (Enterprise Resource Planning).
[22] Khandesh College Education Society, (2018), ERP Professionals [WWW Document]. URL https://dksdc.org/course_details.php?cateid=3&id=22&page=course_details (accessed 10.14.18).
[23] Course Hero, (2015). Finance Accounting General Ledger Fixed Assets payables including vouchering [WWW Document]. URL https://www.coursehero.com/file/p7p6hh0e/Finance-Accounting-General-Ledger-Fixed-Assets-payables-including-vouchering/ (accessed 10.14.18).
[24] NATO, (2018). Defence Planning Process [WWW Document]. NATO. URL http://www.nato.int/cps/en/natohq/topics_49202.htm (accessed 10.14.18).
[25] www.naval-technology.com, 2018 Gerald R Ford Class (CVN 78/79) – US Navy CVN 21 Future Carrier Programme – Naval Technology [WWW Document]. URL https://www.naval-technology.com/projects/cvn-21/ (accessed 10.15.18).

Most used abbreviations:
IoT – Internet of Things
WoT – Web of Things
DRP – Defence Resource Planning
ERP – Enterprise Resource Planning
DoD/MoD – Department of Defence/Ministry of Defence
PPBS – Planning Programming Budgeting System
DRM – Defence Resource Management
PDCA – Plan, Do, Check, Act
RDM – Robust Decision Making
GDP – Gross Domestic Product
NDPP – NATO Defence Planning Process

References:

Георгиев В. (2014), Съвременен инструментариум за оценяване на военната(външната) сигурност, в: Съвременен инструментариум за оценяване на сигурността. Анализ на световния и европейски опит, ИК-УНСС, София, с. 90.

(Georgiev, V. 2014, Savremenen instrumentarium za otsenyavane na voennata (vunshnata sigurnost), v: Savremenen instrumentarium za otsenyavane na sigurnostta. Analiz na svetovnya i evropeyski opit., IK – UNSS, Sofia, s. 90)
Димитров, Д. (2014), Функции на отбраната, в: Глобализъм, регионализъм и сигурност, ИК – УНСС, София
(Dimitrov, D. 2014, Funkcii na otbranata, v: Globalizam, regionalizam i sigurnost, IK – UNSS, Sofia, s. 12.)
Димитров, Н. (2014), Енергийна сигурност и сигурност на енергийните ресурси., в: Съвременен инструментариум за оценяване на сигурността. Анализ на световния и европейски опит.. ИК – УНСС, София с. 90.
(Dimitrov, N. 2014, Energiyna sigurnost i sigurnost na energiynite resursi, v: Suvremenen instrumentarium za otsenyavane na sigurnostta. Analiz na svetovnia i evropeyski opit, IK – UNSS, Sofia, s. 90.)
Иванов, Т. (2014), Централицазия или регионално развитие и сигурност? в: Глобализъм, регионализъм и сигурност, ИК – УНСС, София, стр. 17.
(Ivanov, T., Tsentralizatsia ili regionalno razvitie i sigurnost, v: Globalizam, regionalizam i sigurnost, IK – UNSS, Sofia, p. 17.)
Павлов, Г. (2003), Информационни технологии в отбраата и сигурността. УИ – Стопанство, София.
(Pavlov, G., 2003, Informacionni tehnologii v otbranata i sugurnosta, UI – Stopanstvo, Sofia)
Пудин, К. (2009), Съвременната българска армия. Социално икономически аспекти на нейната професионализация. Авангард Прима, София.
(Pudin, K., 2009, /Suvremennata bulgarska armia. Socialno ikonomicheski aspekti na neynata profesionalizatsia, Avangard Prima, Sofia)
Тагарев, Н. (2014a), Кооперирane в областта на киберсигурността на държавите – членки на НАТО, в: Десет години от приемането на България в НАТО. ИК – УНСС, София, p. 25.
(Tagarev, N., 2014a, Kooperirane v oblastta na kibersigurnostta na durzhavite chlenki na NATO, v: Deset Godini ot Priemaneto na Balgaria v NATO, IK – UNSS, Sofia, p. 25)
Тагарев, Н. (2014b), Заплахи от кибер престъпления, в: Глобализъм, регионализъм и сигурност., ИК – УНСС, София, с. 319.
(Tagarev, N., 2014b, Zaplahi za kiberprestaplenia, v: Globalizam, regionalizam i sigurnost, IK UNSS, Sofia, s. 319.)
Тагарев, Н. (2018), Обучение по киберсигурност (киберсигурност и ядрена сигурност), в: Дигитални измами и киберсигурнаст, ИК УНСС, София.
(Tagarev, N., 2018, Obuchenie v oblastta na kibersigurnostt (Kibersigurnost i yadrena sigurnost) v: Digitalni izmami i kibersigurnost, IK – UNSS, Sofia)
Цветков, Ц. (2004), Иновации и инвестиции в отбраната. Университетско издателство "Стопанство," София.

(Tsvetkov, Ts., 2004, Inovacii i investitsii v otbranata, UI Stopanstvo, Sofia.)
Цветков, Ц. (2014), Оценаване на сигурността в процеса на управление – теоретични и методични въпроси. в: Съвременен инструментариум за оценяване на сигурността. Анализ на световния и европейски опит. ИК – УНСС, София с. 7.
(Tsvetkov, Ts., 2014, Otsenyvane na sigurnostta v protsesa na upravlenie – teoretichni i metodichni vuprosi, Suvremenen instrumentarium za otsenyvane na sigurnostta. Analiz na svetovnia i evropeyski opit., IK – UNSS, Sofia, s. 7.)
Ценков, Ю. (2014), Анализ на обкръжаващата среда при проекти за развитие на въоръженията, в: Глобализъм, регионализъм и сигурност, ИК – УНСС, София, с. 371.
(Tsenkov, Yu., Analiz na obkruzhavashtata sreda i razvitie na vuorazheniyta, in: Globalizam, regionalizam i sigurnost, IK – UNSS, Sofia, s. 371.)
Bartha, P. (2016), Analogy and Analogical Reasoning, in Zalta, E.N. (Ed.), The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University.
Bowen, G. A. (2013), Document Analysis as a Qualitative Research Method. Qual. Res. J. https://doi.org/10.3316/QRJ0902027
Carnes, K., (2014). Zen Ledge, LLC – Business Software Consulting, Charlotte, NC [WWW Document]. ZenLedge LLC. URL http://www.zenledge.com (accessed 10.14.18).
Dewitte, L., (2000). New "smart weapons" and reconnaissance pod certified [WWW Document]. URL http://www.f-16.net/f-16-news-article532.html (accessed 1.5.19).
DonVito, P.A., 1961 The essentials of a planning-programming-budgeting system 21.
Eisenhower, (1961). Eisenhower warns us of the military industrial complex. – YouTube [WWW Document]. URL https://www.youtube.com/watch?v=8y06NSBBRtY (accessed 10.14.18).
Fischbach, J.R., (2010). Managing New Orleans Flood Risk in an Uncertain Future Using Non-Structural Risk Mitigation 283.
Gordon, C.V., Hinkle, W.P., (2011). Best Practices in Defense Resource Management: Defense Technical Information Center, Fort Belvoir, VA. https://doi.org/10.21236/ADA541650
Gupta, H., (2011). Enterprise Resource Planning (ERP): A Technology of Effective Management 9.
Hartung, W.D., (2018). The Military-Industrial Complex Is on Corporate Welfare.
Hooper, J.F., (1968). Planning, Programming, Budgeting System 3.
Lempert, R., Warren, D., Henry, R., Button, R., Klenk, J., Giglio, K., (2016). Defense Resource Planning Under Uncertainty: An Application of Robust Decision

Making to Munitions Mix Planning. RAND Corporation. https://doi.org/10.7249/RR1112
Else, D. LibraryOfCongress, (2017). Origins of the Military-Industrial Complex.
Mehta, A., 2017. Mattis intervened to increase munition buy in FY18 budget request [WWW Document]. URL https://www.defensenews.com/congress/budget/2017/05/23/mattis-intervened-to-increase-munition-buy-in-fy18-budget-request/ (accessed 10.14.18).
Mizokami, K., (2018). F-16 Destroys Another F-16 When Maintenance Crew Accidentally Triggers Gatling Gun [WWW Document]. Pop. Mech. URL https://www.popularmechanics.com/military/aviation/a23793250/belgium-f-16-accidentally-destroys-another-f-16/ (accessed 1.5.19).
Norquist, D.L., (2017). Under Secretary of Defense (Comptroller) > Home > ComptrollerNews [WWW Document]. URL https://comptroller.defense.gov/home/ComptrollerNews.aspx (accessed 10.14.18).
Perkins, T.W. and B., 2018. What is ERP? A guide to enterprise resource planning systems [WWW Document]. CIO. URL https://www.cio.com/article/2439502/enterprise-resource-planning/enterprise-resource-planning-erp-definition-and-solutions.html (accessed 10.14.18).
Publication, P., 2005. The Defence Industry in the 21st Century 44.
Tagarev, N., (2018). Economic & Investment Perspectives in the Digital Society, in: Future Digital Society Resilience in the New Digital Age. Presented at the Future Digital Society Resilience in the New Digital Age, Sofia, p. (Under print).
Tagarev, N., (2015). Threats to Information Security, in: East-West Defence and Security Co-Operation Part 1. UNWE publishing Center, Sofia.
Taleb, N.N., (2018). Skin in the Game: Hidden Asymmetries in Daily Life. Random House, New York.
van Groenendaal, W., 2008 Best Practices in ERP: How good are they? 15.
Yunliang, J., Xiongtao, Z., Qing, S., Jing, F., Ning, Z., 2010. Design of E-Government Information Management Platform Based on SOA Framework, in: 2010 First International Conference on Networking and Distributed Computing. Presented at the 2010 First International Conference on Networking and Distributed Computing, pp. 165–169. https://doi.org/10.1109/ICNDC.2010.42

DEFENCE RESOURCE PLANNING IN THE ENVIRONMENT OF THE INTERNET OF THINGS

Abstract

The problem of this article concern the lack of Defence Resource Planning (DRP) for the future environment of the Internet of Things(IoT). This paper shows the aspect in the DRP in Bulgaria and the probable change in the environment of IoT. The article provides data, cases and examples for comparison. The author shows DRP in Bulgaria in some details, that concerns the analyzed object. Study explains the connection between IoT and DRP. There are some basics about ERP. In this article finds a place the main difference between DRP and ERP. The paper acknowledges the threats and the change of the threats in the IoT. In this article are used several methods for quality analyses that include documentary, process, system case study and analogy methods. This article is one of the first with economic and management approach on this topic – smart devices (that communicate independently through IoT) and their significance for DRP. According to the hypotheses, the main author's conclusion is that the implementation of IoT in DRP will have a major impact on the US-centric military oriented states.

Key words: Defence resource planning, Internet of Things, Threats, ERP.

JEL: B41, F59, M150, D610; O21