2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

Weapons Systems and Cyber Security – A Challenging Union

Robert Koch
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
robert.koch@unibw.de

Mario Golling
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
mario.golling@unibw.de

Abstract: A broad range of weapons systems are in service in forces all over the world. Nowadays, state-of-the-art weapons systems are deployed beside legacy high-value systems that have been used for decades, and will continue to be used for some time. Modern weapons systems can contain hundreds of thousands of chips; each of these chips can be of a sophisticated design, containing billions of transistors, making highly complex systems-of-systems. Elderly weapons systems' service lives are often extended or their performance enhanced due to reduced budget funds or delays in new procurement. Therefore, aged and state-of-the art systems have to function together, not only from a communications prospective, but also from a complete systems integration point of view. Modern Network Centric Warfare scenarios rely upon all of these systems being well integrated and be able to interoperate. This spans an incredibly complex range of sensors, communications systems, and weapons of various ages, opening up countless attack vectors and presenting severe challenges to weapons systems security. The paper analyses the parties involved in today's battlespace, examines the impact of the weapons systems' ages on IT security, and surveys the critical factors for cyber security. Numerous highly dangerous factors are identified and essential necessities and countermeasures are recommended.

Keywords: *weapons systems, COTS, counterfeit chips, network centric warfare, defence electronics, supply chain, cyber war*

1. INTRODUCTION

Nowadays, weapons systems are overwhelmingly complex systems-of-systems, which greatly complicates the analysis of overall system security and increases uncertainty about vulnerability to cyber attack. In addition, while a weapons system as a whole is regularly built on home soil, or at least in close collaboration with partner nations, the integrity of its components is

difficult and costly to assure. For example, the integrated circuits (ICs) used in the computers and communications systems of weapons systems are typically purchased from a variety of sources, often from the lowest bidder. It is exceedingly difficult to levy additional requirements such as monitoring component fabrication or subsystem assembly without incurring significant additional costs. As a consequence, there are often troubling questions about supply chain security. Concerns about the relocation of production from expensive Western countries to lower-priced facilities in Asia arose in the 1990s. First, the loss of intellectual property was feared, but soon the security of highly classified systems equipped with externally made chips was questioned. Because of this, in the early 2000s, the US Department of Defence (DoD) started to look for options to improve the security of sensitive defence systems. Concerns continued to grow after the bombing of a suspected Syrian nuclear installation by Israeli jets in 2007 during Operation Orchard. Because state-of-the-art radar technology was not able to detect the jets, rumours arose that a back door integrated into some chips had been used to compromise the system. While a back door enables potential unauthorised access, another type of hardware-manipulation is the so-called 'kill switch' which can be used to disable a circuit remotely. The 2007 incident greatly boosted worries about possible kill switches within chips in nations' own weapons systems [1].

In order to reduce the risk, the DoD and the National Security Agency (NSA) funded the Trusted Foundry Programme (TFP), for ensuring 'access to microelectronics services and manufacturing for a wide array of devices with feature sizes down to 32 nm on 300 mm wafers' [2]. The program contains 52 trusted suppliers that can establish a trusted supply chain. TFP was completed in 2013 and 'provides national security and programs with access to semiconductor integrated circuits from secure sources' [2]. The programme is able to provide chips for the most sensitive systems, but the complexity of modern weapons systems does not allow the removal of chips from untrusted sources entirely. On the contrary; an investigation in 2011 indicated that 40% of military systems were affected by counterfeit electronics [3]. While efforts within the DoD have improved the situation since 2011, counterfeit parts and the supply chain risks still remains challenging, as a report of the United States Government Accountability Office (GAO) to Congressional Committees highlighted in February 2016 [4].

The trade in counterfeit parts is an increasing threat, opening up different dangers. Counterfeit parts often do not meet the quality requirements of the real products, increasing the risk of malfunction of a weapons system. Counterfeit parts can also increase the risk of back doors and manipulated circuits being present.

While much research has been done to find and improve techniques for the detection of malicious circuits, new and even more dangerous manipulations are possible, and highly sophisticated attacks can be conducted even *below* the transistor level. A worrying example is a recent demonstration of the realisation of a hardware Trojan *below* gate level of an Intel Ivy chip, shown by Becker et al [5]. In contrast to other manipulation techniques such as integrating hardware back doors at gate level which requires about 1300 gates, the authors changed parts of the dopant polarity, and therefore the changes were not detectable on the wiring layers by traditional tests like fine-grain optical inspections or checking against golden chips. Becker was able to reduce the entropy of the integrated random number generator (RNG) from 128 down to

32 bits, enabling easy attacks when the manipulation is known. Testing procedures of the RNG based on NIST guidance are not able to detect manipulations of the generated random numbers. Some cases of back doors implemented in chips are already known, for example the discussion about the Microsemi ProASIC 3 [6] used in military systems and the Boeing 787 Dreamliner [7]. In hindsight, those unwanted circuits are regularly qualified as undocumented debugging functionality. However, for military and highly secure systems, it makes no difference if a hardware back door – which is virtually impossible to detect – was forgotten accidentally or was inserted by purpose.

The remainder of the paper is structured as follows. First, an overview of important characteristics of today's weapons systems is given in section 2, and the impact of Network Centric Warfare on Cyber Security is discussed. In section 3, threats with respect to weapons system and the battlefield are analysed and discussed, while in section 4, possible and necessary countermeasures to reduce the threat to cyber security of weapons systems are presented. Finally, section 5 concludes the paper, highlighting the key takeaways.

2. WEAPONS SYSTEMS

Today's battlespace is filled with an extensive variety of weapons systems of all ages.

A. Elderly weapons systems

The development, commissioning and operation of a weapons system is very expensive. For this reason, such high-value systems are built to be in service for more than 30 to 40 years. While this is a long period of time, it is often extended even further for financial or procurement reasons: economic crises and budget cuts have affected all nations at one time or another, resulting in the cancellation of numerous procurement projects. In addition, the buying process of weapons systems can be very time-consuming. Because of late changes to specifications or issues during the development process, delays of many years are not uncommon in this sector. For example, it was 17 years from foundation of the 'Eurofighter Jagdflugzeug GmbH' in 1986 to the delivery of the first production aircraft in 2003, and the unit costs rose from the originally planned €33.32 million to €138.5 million by 2012 [8]. Such delays also can greatly contribute to the extension of the service life of a weapons system. Due to such developments, the *average* age of the weapons systems of a military force can be several decades, even in modern western forces. For example, the average age of US Airforce aircraft is 27 years, and some fleets like the B-52 bomber, which entered service in 1955, are much older [9]. Therefore, the expected life expectancy of many elements of the United States Air Force (USAF) will be reached if the equipment is not enhanced by modifications [9].

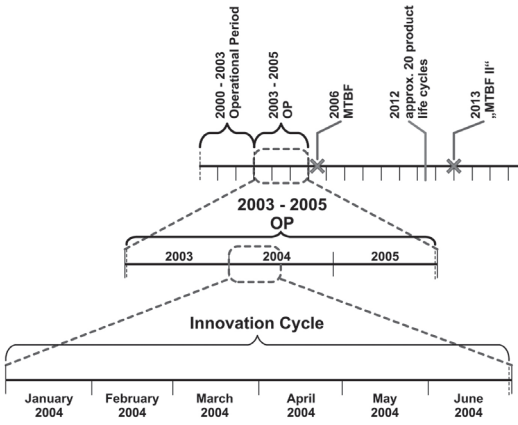
Over the years of operation, the supply of spare parts can also be challenging. Companies might go out of business, change production lines, or produce new and incompatible products. Because of that, and also to maintain availability, mid-life upgrade programmes are conducted one or more times during the life span of a weapons system. More and more commercial-off-the-shelf (COTS) products have to be used to keep systems running and to replace old components which are no longer available [10],[11].

B. State-of-the-art weapons systems

Modern weapons systems are highly complex. They often contain hundreds of thousands of chips, extensive networks, and interconnected sensors and systems. While the military was a driver of technology during the Cold War due to the vast defence budgets for research and development, the peace dividend and several economic and financial crises have necessitated broad budget cuts and reduced overall defence spending. By contrast, the impressive development of Information and Communication Technology (ICT), the Internet and consumer electronics boosted the evolution of the industry to a multi-billion market. Increasingly shorter product and innovation cycles make the commercial market today's driver of technology. To reduce costs as well as to optimise system performance, COTS products are heavily used in modern weapons systems. In turn, the extensive integration of COTS in high-value systems has resulted in new challenges in maintaining the weapons systems over their life cycles. Any attempt to update the ICT components of a weapons system after it is deployed often requires a costly recertification to obtain the authority to operate it. Given the pace of technological advancement, with new ICT being released every few years and weapons systems being designed to operate for a much longer time, it is often cost prohibitive to mandate the update of ICT subsystems in a timely manner.

Looking at the life span of IT components and their mean time between failure (MTBF), and bearing in mind the challenging operational environments such as the broad spectrum of temperatures, material stress caused by high acceleration, or sea disturbance affecting ships, an exchange of these components has to be done at least every ten years. Therefore, a weapons system which is in service for 30 to 60 years requires numerous programmes to refresh it (see Figure 1).

FIGURE 1: HIGH-VALUE SYSTEMS OF THE MILITARY HAVE TO BE IN SERVICE FOR UP TO 40 YEARS OR EVEN LONGER. THEREFORE, ELECTRONIC COMPONENTS LIKE COTS PRODUCTS WITH THEIR TYPICAL MTBF VALUES HAVE TO BE EXCHANGED MULTIPLE TIMES DURING THE LIFE TIME OF THE WEAPONS SYSTEM



MTBF Estimates for Intel Server System SR1630GP

Subassembly (Server in 35oC ambient air)	Server Model SR1630GP MTBF (hours)	FIT (flrs/10^9 hrs)
Intel Server Board S3420GP	208,000	4,808
Power Supply (350W)	400,000	2,500
Cooling fans (Non-redundant)	100,000	10,000
PCI RiserCard	4,100,000	244
Front Panel board	16,000,000	63
Totals without motherboard=	78000	12,806
Totals with motherboard=	56700	17,614

This can cause compatibility issues, and the risk of bringing in manipulated components, counterfeit parts or parts of insufficient quality increases significantly (for example, see [12]).

C. Network-centric warfare scenario

After the end of the cold war, budget cuts forced a more efficient use of funding. While military budgets were reduced, the development, fabrication, operation, and maintenance costs of weapons systems increased steadily. Under these constraints, the best possible use of the limited number of available weapons systems had to be realised. Therefore, the interconnection of all available systems and the appropriate provisioning of any required information at all levels was the answer to maintaining force superiority with a progressively limited, but technically more capable, number of units. This is called Network Centric Warfare (NCW).

The US Navy was one of the first to look at a 21st century battlefield and think of how to use ICT to increase the efficiency of forces [13]. The main consequence of their considerations was the increased integration of individual, previously autonomously acting systems. This technical integration has finally led to the concept of NCW. This is a theory that proposes the application of information age concepts to speed communications and increase situational awareness through networking, and improve both the efficiency and effectiveness of military operations [14]. NCW creates information superiority by means of a network of reconnaissance, command and control, and weapons systems, and thus ensures military superiority across the entire range of military operations (full spectrum dominance). The vision for NCW is to provide seamless access to timely information at every echelon in the military hierarchy. This enables all elements to share information that can be combined into a coherent and accurate picture of the battlefield. This concept of strong and flexible networked military forces allows combat units to be smaller, to operate more independently and effectively, to prevent or reduce fratricide, and to speed up the pace of warfare in comparison to non-networked forces [14]. NCW will also produce an improved understanding of higher command's intent, improved understanding of the operational situation at all levels of command, and an increased ability to tap into the collective knowledge of all forces to finally reduce the 'fog and friction' [14]. While the concept of NCW enables the optimal use of resources, the vulnerability of the overall system rises dramatically: attacking the weakest link of the NCW chain can have catastrophic consequences for its owner, in the worst case rendering a whole military component incapable of action.

3. THREAT ANALYSIS

Having a look at the wide range of weapons systems in today's battlespace and the numerous attack vectors which are connected with them, questions about the most dangerous vulnerabilities arise. In modern warfare, all systems are highly interconnected and gravitate towards NCW scenarios, and a breach of the weakest link can have a severe effect for a whole operation.

A. Old versus new

Because of the mix of elderly weapons systems and those that are state-of-the-art, one might come to the conclusion that older weapons systems are per se more unsecure than newer systems. Although that is often true in that older systems run on older software and may have

challenges with respect to software updates and patches, modern systems have their own problems with outdated software because of the long design and procurement times. Because of mid-life upgrade programmes, old weapons systems are modernised, sometimes with replacement of nearly all their ICT components. Therefore, elderly as well as state-of-the-art systems can contain old as well as new IT components, and have to be treated equally with respect to cyber threats.

B. Defence technological and industrial base (DTIB) capabilities

The capability of the Defence Technological and Industrial Base (DTIB) is another important aspect. The DTIB is the combination of people, institutions, technological expertise, and production capacity used to develop, manufacture, and maintain the weapons and supporting equipment needed to achieve national security objectives [15]. The European Defence Agency defined a strategy for a European DTIB, aiming at strengthening available European capabilities, motivating higher investment, and promoting the broader use of the public procurement regulations of the EU [16]. While Europe has many capable defence companies, components such as electronic semiconductors are often not produced in Europe, but in the Asia-Pacific region [17]. At present, the limited prospects to maintain core IT components of weapons systems are also not addressed explicitly within the DTIB strategy of the EU; in fact, this strongly limits the effectiveness of the European DTIB, and also those of other Western DTIBs that suffer from similar restrictions.

C. Supply chain

While producers in North America slowly stabilise their market share after losing most of it in the nineties and the first decade of this century, Europe's electronic equipment production is still declining, while also China is being challenged by upcoming producers in other Asia-Pacific regions like India and Malaysia [17]. Therefore, the supply chain of IT technology currently presents a severe danger to the security of weapons systems. Because of the complex and globally distributed chip design ecosystem, a multitude of companies and countless people are involved in the building process, from specification to shipping [18]. Driven by the optimisation of business processes, cost-reduction in manufacturing, outsourcing, and globalisation, building a chip nowadays involves a huge number of parties at every step: specification, design, manufacture, and testing. The various steps are distributed between numerous companies. Nowadays, even parts of a chip can be reused or purchased from other companies and the huge number of people involved during chip creation enables a growing threat of design corruption [18].

All steps of the building process can be manipulated to a greater or lesser extent. Some examples of this include: manipulation of specifications; [19] influencing the design process by introducing back doors; forgetting to remove debugging functionality – see the discussion about the hardware backdoor in the Actel/Microsemi ProASIC3 chips; [6] and executing very small changes during chip manufacture (for example, adding a back door requires about 1300 gates, [20] while in contrast, the recent SPARC M7 contains 10 billion transistors – therefore as few as 0.000013% gates have to be added; these are virtually undetectable for today's typical test suites which are able to identify accidental design flaws effectively based on calculus of

probabilities, but which struggle to find intentionally hidden alterations made by a skilled designer [18]).

In addition to these possibilities, an increasing market exists for the sale of counterfeit parts. In 2012, worldwide trade in counterfeit semiconductors reached $169 billion [21]. As this is a lucrative business, a strong further increase can be assumed. Counterfeits endanger weapons systems in two ways: the poor quality typically cannot meet the original specification; and the risk of there being manipulated circuits increases dramatically. In 2012, it was reported that 'a record number of tech products used by the US military and dozens of other federal agencies were fake. That opens up a myriad of national security risks, from dud missiles to defective airplane parts, to cyberespionage' [12]. For detailed examples of supply chain vulnerabilities and resulting risks to DTIB, see [22].

D. Compatibility and maintenance supportability

The long life of weapons systems can also be challenging when components which have to be replaced are no longer available on the market. Often, new products are not compatible with older ones; but even if a newer product is compatible, various problems may occur in practice (for example, while SCSI components should be backwards compatible, it should be possible to use an Ultra-160 SCSI disc on the bus of a SCSI-1 host adapter). Even though this is possible in theory, device compatibility is often reduced in practice, such as when there are different signalling implementations even within the same standard. In the worst case, obsolete components have to be installed in a weapons system to keep it running, increasing costs as well as the danger of counterfeit electronics.

Also, mass market electronics are typically not optimised for radiant emittance further than the basic requirements of electromagnetic compatibility dictate (for example, the EU directive 1999/5/EC on radio equipment and telecommunications terminal equipment [23] or directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility [24]). With respect to security-related systems, such directives are often not sufficient: for example, electromagnetic compatibility is defined in Article 2 of 2004/108/EC as: 'the ability of equipment to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to other equipment in that environment'. No threshold values are given by the directives, causing possible trouble when systems have to be replaced but new products cannot fulfil function parameters like the old one.

Today's weapons systems are threatened by fake microelectronics and possible manipulations of the hardware, limited supply of spare parts, and counterfeit parts. While real examples are naturally highly classified, the real-world danger can be recognised by examples like manipulated processors [6], the recent discussion about back doors in widely-used network equipment [25], or statements. For example, IEEE Spectrum wrote in 2008, that:

> 'according to a US defence contractor who spoke on condition of anonymity, a "European chip maker" recently built into its microprocessors a kill switch that could be accessed remotely [...] If in the future the equipment fell into hostile hands, "the French wanted a way to disable that circuit," he said' [1].

4. COUNTERMEASURES

The most important precondition for defining adequate countermeasures is to accept the current situation and the undesirable, but in the medium term unchangeable, reality. It is neither possible to exchange the entire hardware layer to a trusted one, nor to build an all-embracing DTIB. One must act on the assumption that the already deployed hardware-layer is not trustworthy. Therefore, pre-planned reactions for a worst-case scenario are elementary.

A. Emergency planning

The defence capabilities and weapons systems of a nation state are of interest to other nations and non-state actors. The components of today's complex weapons systems and their innermost component parts, especially the chips controlling sensors, communication systems, data exchange and weaponry systems, are often COTS products delivered by a lengthy supply chain involving hundreds of companies and thousands of people. Reactions and countermeasures must be developed and installed on all units and elements as well as at all management levels. This includes the creation of emergency and disaster plans. In order to keep the associated complexity manageable, vital components have to be identified and addressed.

B. Risk management

An organisation-wide risk management must be established, encompassing all units and management levels, but which also has to be integrated in the procurement and planning processes. For this purpose, the standards published by the International Organisation for Standardisation (ISO), can be referred to: ISO 31000:2009 (Risk management – Principles and guidelines) and IEC 31010:2009 (Risk management – Risk assessment techniques). COBIT 5 for risk can be used to implement a holistic and organisation-wide risk management regime. This includes guidance on how to manage the risk to levels, how to implement extensive measures, and how to enable stakeholders to consider the cost of mitigation and required resources as well as other aspects such as setting up an appropriate risk culture [26].

C. Supply chain

Today, specific threats exist not only in the production process of chips, but in particular during the design phase. Therefore, all steps from specification to shipping have to be taken into consideration to establish a more trustworthy supply chain. However, the economic reality, with its globalised business processes, must be accepted and be reflected in an appropriate strategy for dealing with the supply chain. For example, by boosting and funding research for new processes and technologies for securing design tools and development.

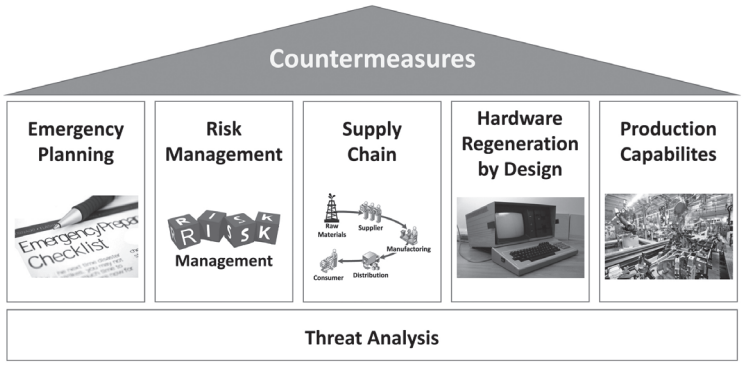
D. Hardware regeneration by design

Looking at individual weapons systems, procurement processes have to be adapted to reflect the requirements of operating short-lived COTS hardware in long-lasting high-value weapons systems. Therefore, not only an exchange of semiconductor components on a regular basis is necessary, but also the provision of concepts of how to deal with compatibility issues, methods for the detection of counterfeit or manipulated chips, and migration strategies for the system core elements in case of severe problems of incompatibility with new hardware.

E. Production capabilities

A strengthening of the European DTIB is necessary to provide all essential components of weapons systems, including the production of semiconductor electronics for the most sensitive systems. This includes a further strengthening of companies already producing crypto- and specialised chips for high-security systems, as well as updating the strategy for the European DTIB, and the creation of an own production capacity, following the example of the TFP.
Figure 2 summarises the identified fields of action which are required to improve the security of weapons systems, and attenuate worst-case scenarios.

FIGURE 2: FIELDS OF ACTION FOR AN IMPROVEMENT OF THE SECURITY OF WEAPONS SYSTEMS AND ATTENUATING WORST-CASE SCENARIOS



5. CASE STUDY: SUPPLY OF SEMICONDUCTORS IN THE US MILITARY

In order to demonstrate the increasing challenges with respect to the supply of semiconductors in US military electronics, this section presents a case study, highlighting the effects achievable by applying the proposed countermeasures. While the US is still a global leader in research and development (R&D) in the semiconductor industry, ever growing proportions of the fabrication take place in the Asia-Pacific region, and this is likely to grow over the coming years. A situation that Brigadier General (ret.) John Adams summarises as follows:

> 'The Chinese telecommunications industry has grown rapidly, with Chinese-manufactured telecommunications equipment spreading swiftly due to below-market prices supported by funding from the Chinese military. The widespread use of military-funded Chinese equipment in conjunction with the shrinking market share of trusted US telecommunications firms increases the likelihood that kill switches or back doors will be inserted into key communications infrastructure, jeopardizing the integrity of sensitive defence-related communications' [22].

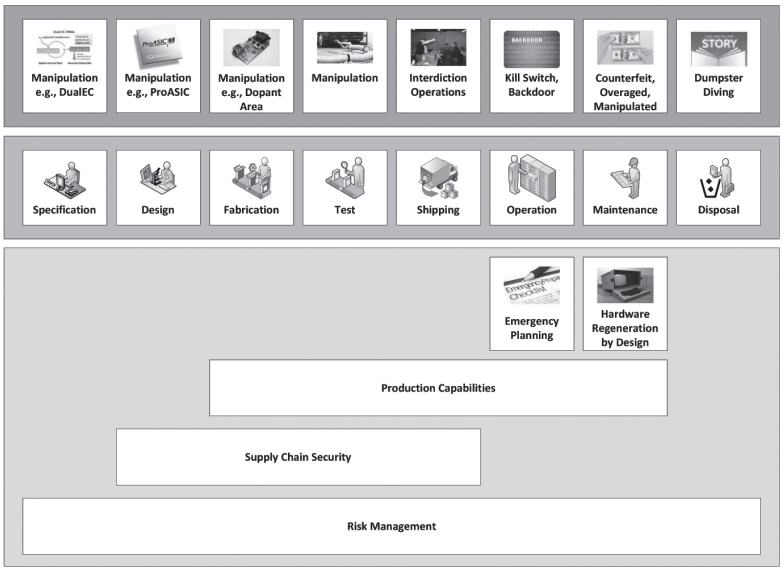
Chinese companies like Huawei or ZTE have a large, constantly increasing market share, providing important network equipment to various customers including military systems and communications. Manipulated circuits containing kill switches or back doors could easily be introduced into systems and networks, but locally designed circuits made by trusted companies using offshore factories can also be infiltrated in that way. For example, telecommunications equipment like the AN/VRC-92A vehicular radio set or the AN/PSC-2 radio may be affected by untrustworthy components (e.g., see [22]). Having a look at the proposed countermeasures, the following measures will be effective in case of manipulated circuitry which may already be used in operational equipment:

(i) Extensive and realistic emergency planning must be able to provide all necessary guidelines to sustain an outage of the respective equipment. For example, if a communication system of manufacturer A is failing (because of the activation of a kill switch), another available device built by manufacturer B and preferably based on different architecture must be able to take over the services. The emergency plan must contain all information to enable the operator to execute all necessary steps (in manifold scenarios) as fast as possible and must be exercised regularly.
(ii) Appropriate risk management must provide guidelines, including the consideration of circumstances that may influence the operation or security. For example, having a manipulated processor within a system where the manipulation cannot be exploited (e.g., an isolated system without any connectivity) does not impose any limitations, while a system connected to the Internet may be highly vulnerable.
(iii) The building of fabrication capabilities can also be used to replace untrusted components of endangered systems that are already in use.

Applying all countermeasures, the risk of introducing manipulated circuitry can be reduced by providing fabrication capabilities for the most essential and restricted systems, and increasing the supply chain security to reduce possible manipulations (e.g., see [27]). Especially for new procurement projects, the necessity of regular hardware regenerations must be incorporated by design. For example, the specification and selection of components must be done in a way that common, long-lasting and open standards (like for example IPv4/6) are used, enabling a replacement of components with minimal adjustment, even when the original supplier is out of business or the product line was phased out. Because of the increased risk of counterfeit parts, novel compatible parts also should be used if original parts are only available from untrustworthy sources.

Figure 3 gives an overview of the obtained effects with respect to the supply chain, when all countermeasures are applied.

FIGURE 3: HOLISTIC RISK MANAGEMENT



6. CONCLUSION

The modern battlefield is a complicated environment where numerous highly complex weapons systems which are a broad mixture from several generations, and variations of electronic equipment of different ages interact. This generates special demands on cyber security, but these sensitive systems are increasingly vulnerable to cyber attacks, as examples like Operation Orchard have shown. Based on the relocation of production capabilities to lower-priced countries and the globalisation of chip production, numerous threats of attacks or manipulations are endangering modern weapons systems. Because of the strongly diverging life cycle times of COTS products and military high-value systems, and the prevalence of counterfeit electronics, the required exchange of hardware components on a regular basis opens up significant challenges. While elderly and modern weapons systems are facing these same challenges and threats, the total risk increases dramatically within a NCW scenario.

Therefore, organisation-wide emergency-management and risk-management is vital. Each unit as well as all management levels must be able to react promptly in case of attack executed at the hardware layer. A strengthening of the European DTIB capabilities especially in the field of semiconductors for sensitive systems is necessary, and new concepts and techniques for improving the security of the supply chain for electronic products from the world market have to be developed. While this will have huge costs, the TFP of the United States shows that building up secure microelectronics manufacturing capacities is viable. Having a look at the

procurement processes, the integration of hardware-regeneration concepts on a regular base is essential.

ACKNOWLEDGMENTS

This work was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

REFERENCES

[1] S. Adee, 'The hunt for the kill switch,' *Spectrum, IEEE*, vol. 45, no. 5, pp. 34–39, 2008.
[2] C. Ortiz. Dod trusted foundry program. [Online]. Available: http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/.
[3] J. Mick. US GOA [sic.]: 40 Percent of Defense Supply Chain Damaged by Chinese Parts. [Online]. Available: http://www.dailytech.com/US+GOA+40+Percent+of+Defense+Supply+Chain+Damaged+by+Chinese+Parts/article21937.htm.
[4] M. A. Mak, 'Counterfeit parts - DOD needs to improve reporting and oversight to reduce supply chain risk,' United States Government Accountability Office, Tech. Rep., 2016, gAO-16-236, Report to Congressional Committees. [Online]. Available: http://www.gao.gov/assets/680/675227.pdf.
[5] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, 'Stealthy dopant-level hardware Trojans,' in *Cryptographic Hardware and Embedded Systems-CHES 2013*. Springer, 2013, pp. 197–214.
[6] S. Skorobogatov and C. Woods, Breakthrough silicon scanning discovers back door in military chip. Springer, 2012.
[7] C. Arthur. Cyber-attack concerns raised over Boeing 787 chip's 'back door'. [Online]. Available: http://www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-boeing-chip.
[8] M. Freund, D. Klager, J. Mallien, and D. Neuerer. Totalschaden mit Ansage. [Online]. Available: http://www.handelsblatt.com/politik/deutschland/ruestungsflops-der-bundeswehr-die-entwicklung-des-eurofighter/8232292-3.html.
[9] D. L. Wood, '2016 index of US. military strength,' The Heritage Foundation, Tech. Rep., 2015. [Online]. Available: http://index.heritage.org/military/2016/resources/download/.
[10] S. Kosiak, Buying Tomorrow's Military: Options for Modernising US Defense Capital Stock. Center for Strategic and Budgetary Assessments, 2001.
[11] L. O. Association. Aging weapons systems. [Online]. Available: http://atloa.org/wp-content/uploads/M1_slides.pdf.
[12] D. Goldman. Fake tech gear has infiltrated the USgovernment. [Online]. Available: http://security.blogs.cnn.com/2012/11/08/fake-tech-gear-has-infiltrated-the-u-s-government/.
[13] D. S. Alberts, 'Information Age Transformation: Getting to a 21st Century Military (revised),' DTIC Document, Tech. Rep., 2002.
[14] C. Wilson, 'Network centric operations: background and oversight issues for congress.' DTIC Document, 2007.
[15] W. Slocombe, 'Adjusting to a new security environment: The defense technology and industrial base challenge - background paper,' US Congress, Office of Technology Assessment, Tech. Rep., 1991.
[16] EDA Steering Board, 'A strategy for the European defence technological and industrial base,' European Defence Agency, Tech. Rep., 2007.
[17] E. Publications, 'World electronic industries 2012-2017,' Electronics.ca Publications, Tech. Rep., 2014. [Online]. Available: https://www.electronics.ca/store/world-electronic-industries.html.
[18] J. Villasenor, 'Compromised by design? securing the defense electronics supply chain,' *Brookings Institution Report*, Nov, 2013.
[19] D. J. Bernstein, T. Chou, C. Chuengsatiansup, A. Hülsing, T. Lange, R. Niederhagen, and C. van Vredendaal, 'How to manipulate curve standards: a white paper for the black hat,' Cryptology ePrint Archive, Report 2014/571, Tech. Rep., 2014.
[20] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, 'Designing and implementing malicious hardware.' *LEET*, vol. 8, pp. 1–8, 2008.

[21] L. Dignan. Counterfeit chips: A $169 billion tech supply chain headache. [Online]. Available: http://www.zdnet.com/article/counterfeit-chips-a-169-billion-tech-supply-chain-headache/.
[22] J. Adams and P. Kurzer, Remaking American security: Supply chain vulnerabilities & national security risks across the US defense industrial base. Alliance for American Manufacturing, 2013.
[23] 'Directive 1999/5/ec of the european parliament and of the council of 9 march 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity,' 1999. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0005.
[24] 'Directive 2004/108/ec of the European parliament and of the council of 15 December 2004 on the approximation of the laws of the member states relating to electromagnetic compatibility and repealing directive 89/336/eec,' 2004. [Online]. Available:http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:390:0024:0037:en:PDF.
[25] H. Böck. Juniper wegen Hintertüren in Erklärungsnot. [Online]. Available: http://www.golem.de/news/zufallszahlengenerator-juniper-wegen-hintertueren-in-erklaerungsnot-1601-118457.html
[26] Isaca, *COBIT 5 for Risk*. Isaca, 2013, ASIN: B01A1MXZ30.
[27] Ghadge, Abhijeet, Samir Dani, and Roy Kalawsky.'Supply chain risk management: present and future scope.' The International Journal of Logistics Management 23.3 (2012): pp. 313-339.