Next Big Thing in Big Data: the Security of the ICT Supply Chain

Tianbo Lu[1,2], Xiaobo Guo[1], Bing Xu[1], Lingling Zhao[1], Yong Peng[3], Hongyu Yang[2]
[1]School of Software Engineering Beijing University of Posts and Telecommunications
Beijing, China
[2]Information Technology Research Base of Civil Aviation Administration of China, Civil Aviation University of China,
Tianjin, China
[3]China Information Technology Security Evaluation Center
Beijing, China
lutb@bupt.edu.cn; gxbbest@126.com; xub@bupt.edu.cn

***Abstract*—In contemporary society, with supply chains becoming more and more complex, the data in supply chains increases by means of volume, variety and velocity. Big data rise in response to the proper time and conditions to offer advantages for the nodes in supply chains to solve prewiously difficult problems. For any big data project to succeed, it must first depend on high-quality data but not merely on quantity. Further, it will become increasingly important in many big data projects to add external data to the mix and companies will eventually turn from only looking inward to also looking outward into the market, which means the use of big data must be broadened considerably. Hence the data supply chains, both internally and externally, become of prime importance. ICT (Information and Telecommunication) supply chain management is especially important as supply chain link the world closely and ICT supply chain is the base of all supply chains in today's world. Though many initiatives to supply chain security have been developed and taken into practice, most of them are emphasized in physical supply chain which is addressed in transporting cargos. The research on ICT supply chain security is still in preliminary stage. The use of big data can promote the normal operation of ICT supply chain as it greatly improve the data collecting and processing capacity and in turn, ICT supply chain is a necessary carrier of big data as it produces all the software, hardware and infrastructures for big data's collection, storage and application. The close relationship between big data and ICT supply chain make it an effective way to do research on big data security through analysis on ICT supply chain security. This paper first analyzes the security problems that the ICT supply chain is facing in information management, system integrity and cyberspace, and then introduces several famous international models both on physical supply chain and ICT supply chain. After that the authors describe a case of communication equipment with big data in ICT supply chain and propose a series of recommendations conducive to developing secure big data supply chain from five dimensions.**

Keywords: Big data, ICT supply chain model, Information Security, System Integrity, Cyberattacks

I. INTRODUCTION

Big Data is initially driven from service supply chain management (SCM) such as finance, healthcare, tourism, telecommunication, information technology etc. It is reported that, since the 1980s, the per-capita capacity to store information has approximately doubled every forty months.

There is a close relationship between ICT supply chain and global big data commerce. Supply chain links and optimizes all aspects such as suppliers, manufacturers, distributors and retailers. A large part of their information gathering, decision making and mutual interaction is pushed by means of big data, which can be used to anticipate through advanced analytics, do listening ,testing and learning, do sensing before responding, help adapting to changes, deliver products safety, encourage digital manufacturing and digital services and promote supply chain visibility[1]. ICT supply chain is the carrier of big data, as it is responsible for producing all the software and hardware related to the production, storage and application of big data. So the security problems of ICT supply chain must have something with big data security. Any disruptions in supply chain can cause huge loss. However, many companies were not aware of the importance of supply security and they only relied on luck to resist disastrous supply chain disruption.

To start seriously looking at supply chain security, what supply chain is must be defined. Supply chain is a system of organizations, people, processes, technology, information and resources in moving a product or service from the supplier to the customer [2]. Physical supply chain is the sum of the activities to promote the circulation of commodities. In the circulation process, the goods, after production and assembly, flow from the source (raw materials or components) to many warehouses and distribution center, and eventually reach the customer. This process is usually realized through retail stores, now more and more products are direct distributed to individual homes or enterprise. Physical supply chain also includes product back due to rework or warranty. In addition to the physical circulation of commodities, data transfer and financial transactions are also included. More and more companies become increasingly aware of the importance of the supply chain to the overall success of the business. However, the supply chain is very complex, including suppliers, buyers, manufacturers, warehouse and transportation managers, wholesalers, retailers and customers. As an independent part of the supply chain, each of them has a decisive function. Any collapse or failure of any link in the supply chain will reduce the effectiveness of the entire system.

978-0-7695-5137-1/13 $26.00 © 2013 IEEE
DOI 10.1109/SocialCom.2013.172

ICT supply chain is the full set of key actors included in the network infrastructure, including end-users, policy makers, procurement specialists, systems integrators, network provider and software/hardware vendors which produce big data. Through the interaction of organizational layer and process layer, these users/suppliers plan, build, manage, maintain, and protect the network infrastructure[3]. Similar with physical supply chain, cyber supply chain is an end-to-end process. The progress begins with software developers, whose duty is similar to the supplier on the entity supply chain. The roles of procurement departments, production and distribution managers on the entity supply chain are extremely similar with the roles of policy makers, system integrators, hardware/component developers and software vendors on the cyber supply chain. Consumers on the physical supply chain are the same with operators/end users on the cyber supply chain.

Even many countries or organizations pay more and more attention to supply chain, incidents related to it still Occur frequently. In 2010, a worm called "Stuxnet" embedded in the Siemens industrial control software designed for nuclear power plants penetrated the Iran nuclear plant at Natanz through the ICT supply chain, leading to the delay in the generation of the nuclear power plant [4]. In January, 2013, due to the battery components of the Boeing 787 airliner produced in Japan failed repeatedly, nearly all the terminal countries in the Boeing 787 supply chain such as the United States, Japan, Chile and India halted the flight of this type aircraft and grounded check, resulting in a significant impact on safety of passengers and airlines operation [5].

ICT supply chain is the supply chain of supply chain. If it is destroyed, the physical supply chain depending on it will also be destroyed, regardless of whether themselves have been attacked. Due to the popularization of ICT in worldwide network environment, supply chains are likely to be destroyed as long as they exist, and therefore the ICT supply chain security has attracted wide attention.

II. ICT Supply Chain Security

It is necessary to understand that ICT Supply Chain is facing many kinds of security problems. As we can see from Figure 1, it is a model that provides three aspects to study ICT Supply Chain Security. The three aspects are Information Management, ICT System Integrity and Cyberspace.

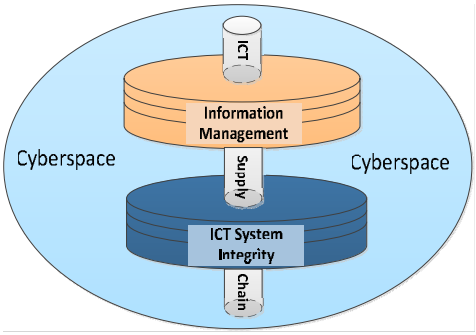

Figure 1. Three aspects to assure ICT supply chain security

A. The Information Security of ICT Supply Chain

"In the modern world, the supply chain is information. When something has been ordered ... where it's going to be manufactured and by whom and how much and what specifications ... all are either on the Internet or in private data systems that are subject to being hacked and invaded." said by former Virginia Governor James S. Gilmore, III [6].

Supply chain links and optimizes all aspects such as suppliers, manufacturers, distributors and retailers. All node enterprises of the supply chain consist of the integration of a core competency of dynamic alliance by means of information technology based on a common goal [7]. Members within the organization can collaborate quickly in response to market demand and optimize the organization's goals by sharing information with the use of big data [8]. Computer network connectivity and openness to the sharing of resources and communication brings maximum convenience, at the same time, network security become more important and urgent issues. Dynamic supply chain alliance Extract is connected with the Internet, this connection provides non-allied enterprises a very easy way to spy on the company's virtual private network, access or tamper with the internal information and resources.

The supply chain is actually an extremely complex information management system, and products and services provided by ICT supply chain are used to transfer and carry large amounts of data. Companies in the supply chain often need to share inventory information, the demand for information, sales information, forecasts, customer data and technical documentation and so on, to share the information which is critical to individual enterprise and the entire supply chain, network equipment may be needed, if any node is attacked, all enterprises in the supply chain will be affected..

B. The Integrity of ICT Supply Chain

ICT supply chain activities began with acquirement, but rarely acquirement system can track the final product completely in the supply chain, acquirers often only know about the participants in contact with him directly and know nothing about sub-suppliers in the supply chain. Any secondary supplier can insert loopholes in software or hardware it provided, waiting for an opportunity to destroy system.

In the context of information security, integrity means that the data has not been altered in an unauthorized manner, degraded or compromised. Within the software context, SAFECode defines integrity as "ensuring that the process for sourcing, creating and delivering software contains controls to enhance confidence that the software functions as the supplier intended" [9]. In ICT in general, integrity is a complex notion linked to the concepts of security assurance and trust (we trust systems when they behave and perform in the expected manner). In the end, the goal is to provide ICT products that meet the original and/or agreed upon specifications [10][11].

The ICT supply chain is faced with many security issues, many of which may cause big data security problems: the malicious logic on hardware and software, installation of counterfeit modules, problems in production process or important product and service distribution process, inadvertently installed hardware and software vulnerabilities.

These “logic bomb”, “back door” and “spyware” inserted in microchips and circuit logic, firmware and software can destroy or subvert the supply of spare parts, which could allow an attacker to control the entire system and to read, modify or remove sensitive information, interrupt the operation of system, or attack other organizations, or even destroy the system, resulting in significant losses [12][13].

C. The Cyberattacks in ICT Supply Chain

In anonymous cyberspace, people can work together to plan and coordinate the implementation of an action. Before, in, or after the attack, attackers may have never met. Due to the development and popularization of the Internet technology, an attacker can launch an attack in many ways, including the design, manufacture, transfer, delivery, installation, maintenance or upgrades. The threat to ICT supply chain is largely caused by the network. Global supply chain increasingly depends on technology, and vulnerability of the supply chain is rising confronting with network threat. In turn, supply chain connectivity also expands the existing network security threats seriously[14].

The asymmetry of cyberspace threats is more and more obvious. Only being successful at any location and in any event, can defenders successfully maintain the security of the network, but the attacker can achieve great success if he can make a successful attack in any one location or event. The asymmetry of cyberspace threats in ICT supply chain make the big data encounter unprecedented crisis [14].

III. The Existing Supply Chain Security Model

It is because of the presence of the security problems in all aspects of the ICT supply chain, which may further penetrate to big data project, we need to implement security measures. So far, models covering the entire ICT supply chain operations have not been developed, but several famous supply chain models from different angles have been promulgated. This paper provides a description of five famous models.

A. *Supply Chain Operations Reference Model*

The supply chain operations reference model (SCOR) is a supply chain management approach developed and authorized by the international Supply-Chain Council (SCC).Its basic idea is to integrate business process reengineering, benchmarking and best practices into a multifunctional model [15].

- Process Simulation

With the help of a recognized process definition, SCOR can be used to describe any supply chain in means of process simulation module, no matter how simple or complex it is. In this way, different industries can be linked together. Including five distinct management processes, shown in Figure 2: Plan, Source, Make, Deliver and Return, SCOR is to provide a standard method to measure supply chain performance and to make comparisons between different enterprises with a set of recognized metric scale [16].

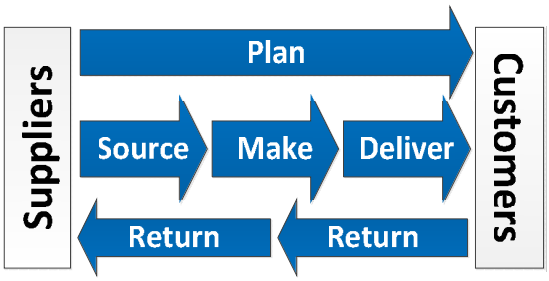

Figure 2. SCOR management process [16]

SCOR model in accordance with the process definition can be divided into three levels, and each level can be used to analyze the operation of the enterprise supply chain.

The first layer, which is the starting point to create a competitive target, consists of five basic processes: plan, source, make, delivery and return. It defines the scope and content of the SCOR and determines the basis of enterprise competitive performance goals [16].

The second layer is called the configuration layer, composed by multiple core processes of the supply chain. Enterprises choose what they need from standard process units defined by the layer to build the actual or ideal supply chain. Each product or product model can have its own supply chain [16].

The third layer is the decomposition layer, which gives the details of the process elements in each process classification in the second layer, to provide the information for enterprises to develop a successful plan, to set a goal of improving the supply chain as well as to improve the performance of the supply chain. It supports all business processes in the second layer. Each second layer process consists of multiple third layer process [16].

- Metrics

The performance attribute refers to the characteristics of the supply chain. It allows us to analyze and assess supply chain with competitive strategy. This is like if you want to describe a timber, you need to use the long, wide and high features to describe, so does the supply chain. Otherwise, it is extremely difficult to compare an enterprise who selects low-cost suppliers with one who selects high reliability suppliers.

- Best Practices

After the supply chain performance has been assessed and the performance gap has been identified, the next important step is to determine what kind of action can be used to fill the gap. In SCOR, “Best practices” is a method with structuring, confirmed and repeatable features, which is used to give positive impact on the ideal operation results. SCOR offers more than 430 operational practices, which are all from the actual experience of the SCC members.

SCOR is the first standard supply chain process reference model and it is a supply chain diagnostic tool that covers all industries [17]. It is conducive to promoting the internal and external supply chain cooperation and the level process integration, by means of giving relationships between processes

(such as planning and acquisition, planning and manufacturing). It enables accurately communication between enterprises, objective performance assessment, the determination of performance improvement.

B. Cyber Supply Chain Assurance Reference Model

In order to support the president's Comprehensive National Cyber Security Initiative (CNCI), SAIC and SCMS of the Robert H. Smith School of Business, University of Maryland (UMD) at College Park, collaboratively undertook a research initiative to develop a Cyber Supply Chain Assurance Reference Model. Cyber is a high-speed channel of big data and an important operating environment of ICT supply chain, so it is very necessary for us to get to know this model[18].

It stresses there is a need to implement security measures in cyber supply chain life cycle and to make an effective integration between the field of network security and supply chain risk management. It research sought to fuse together the fields of cyber security and supply chain risk management by applying proven supply chain practices to this evolving cyber domain [18].

This research first gives a description of network supply chain ecosystem and introduces each key actor's role: policy makers, ecosystem acquisition specialists, system integrators, software developers, hardware/component developers, network providers, operators/end users. Then it defines the cyber supply chain assurance model which includes strategic relations, organizational structure, operating parameters and scope of application [18].

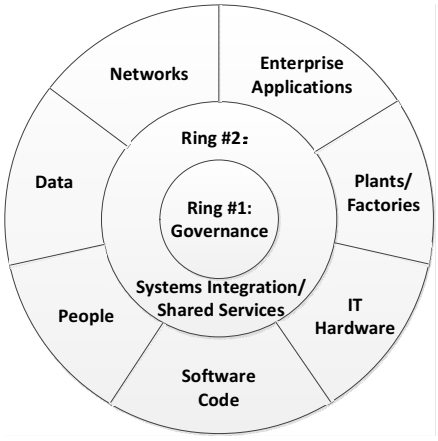

Figure 3 Cyber Supply Chain Assurance Reference Model [18]

This model is the process system, composed by three nested rings, as shown in Figure 3. The three rings represent different aspects of the planning and operational control to solve requirements of defense in depth in the life cycle of system development and breadth defense in cyber supply chain. The three rings are as following:

Ring 1 (Management): The ring mainly solves the related issues of the ICT supply chain security risk management, and clears that the requirements of cyber supply chain risk management and customers is the driving force of the "hub" organization, and customer represents management functions, which is the core ring of the "hub" [18].

Ring 2 (System integration and shared services): The ring is mainly to solve the security issues of operation and maintenance services in the ICT supply chain. Systems integrators, which are in the second ring near the center, are on behalf of the command functions of the cyber supply chain. The goal of this ring is to show the customer requirements, and the role is the "arm" of the "hub" service or the "conductor" to achieve highly synchronized appointing, designing, building, maintaining and processing activities [18].

Ring 3 (Actions and Practice): The requirements to be solved in this level include the best practice processes of specific action role and integrated network/tangible assets management, also include the development, collection and distribution of the reference measures which are using by organization currently threaten by strong global ICT supply chain risk. This ring is mainly to address the security issues in ICT supply chain itself, or in ICT products manufacturing, such as the security issues in software supply chain and hardware supply chain. Suppliers ring manages a wide range of physical devices, workplaces and virtual intellectual property [18].

Based on the actors' common interests, this model not only makes enterprise itself be in charge of the upstream enterprises, but also for the whole supply chain. The most important goal of the ICT supply chain security assurance model is: definite a series of related principles/measures and its organizational framework. If these principles/measures are effectively implemented, the construction and operation of the cooperating agencies, the integrity and quality of ICT supply chain system, and the highly integrated control implementation will become reality.

C. Pricewaterhousecoopers - Supply chain security dimension model

Supply chain security dimension model is proposed in "Transport and logistics 2030, volume four", which responses to the problem of supply chain security in the context of globalization. As shown in Figure 4, this model takes a comprehensive look across five dimensions of supply chain security: Personnel security, ICT security, Process security, Physical security and Security partnerships, and offers suggested activities for each area, supported by a key performance indicator (KPI) and the time horizon for when the activity could be put into practice [19].

There is a wide range of possibilities for improving supply chain security. This model sketches out a range of possible options. But the list is not exhaustive, and not every activity will be a good fit for every organization, particularly as existing legislation varies around the world. It should, however, serve as a pragmatic starting point for thinking creatively about how you can optimize your security profile. It can also help promote discussion with supply chain partners about how to work together to improve the security of shipments throughout the entire supply chain.

Figure 4. Pricewaterhousecoopers - Supply chain security dimension model[19]

D. NIST-System Development Life Cycle Model

NIST-System Development Life Cycle Model is proposed by the U.S National Institute of Standards and Technology (NIST) in its special publication NIST SP 800-64. It first describes key security roles and responsibilities in most information system development, as shown in Figure 5. Then it fits security measures into all the phases of system development life cycle model (SDLC) [20].

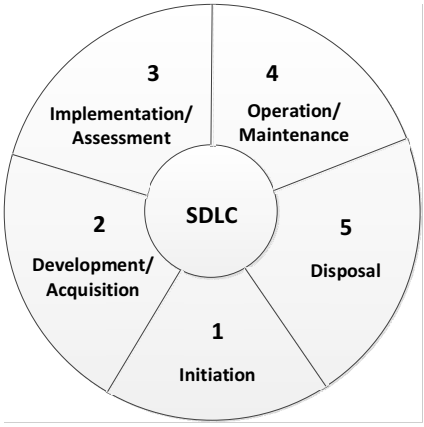

Figure 5.NIST-System Development Life Cycle Model [20]

Initiation requirement: Initiation encompasses the activities that are used to identify the different requirements from all stakeholders, including stakeholders, stakeholder interviews, use cases, and perhaps some basic prototyping. In the end, all the requirements should be identified and thoroughly understood. Development and Acquisition: During this phrase, the functional and technical requirements are changed into detailed plans. Results from interviews, use cases, and mock ups are transformed into sequence diagram or activity diagrams. Implementation and assessment: All the results produced in the two previous phases are changed into application code by software developers and this is the implementation. The assessment includes verifying user functionality through user acceptance testing, quality assurance testing, load testing, and other types of technical test and it is used to ensure that everything is working as expected. Operations and Maintenance: This phrase is used to keep the system working properly. It can include the activities of maintenance on hardware, patch management and fault remediation. User functionality enhancement is not included and additional functionality requires entering the requirements analysis phase again. This phase continues as long as the system exists in a production environment. Disposal: Disposal occurs when the system is replaced or the functionality is no longer needed. During this phase, the system separate itself from production, making it no longer available and accessible to the users [20].

E. The ICT SCRM Community Framework

Following the first report of Maryland University, the ICT Supply Chain Risk Management (SCRM) community framework, which includes three lays, namely risk governance, system integration and operation, is introduced in the second report. This framework comes from three famous above-mentioned models, namely the Supply Chain Operations Reference model, the Cyber Supply Chain Assurance Reference Model, and the NIST-System Development Life Cycle Model. This framework includes two functions which are defense in depth and breadth. Defense in breadth covers clients, acquirers, integrators, suppliers and the key processes between them. Defense in depth is concentrated, which covers risk management, system life cycle management and operation management. These two functions provide a comprehensive ICT SCRM controls.

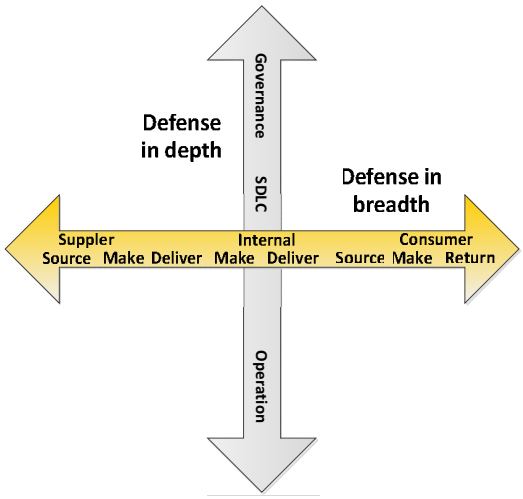

Figure 6. Defense in depth and defense in breadth [21]

In this framework, ICT SCRM is emphasized from two dimensions namely the vertical dimension and horizontal dimension which is presented in Figure 6. Clearly, the strength of cyber supply chains relies on the interdependencies between SDLCs across the supply chain. Thus, operational strategies must operate on two axes. Vertically, the ecosystem requires defense in depth within the SDLC. Horizontally, the ecosystem needs defense in breadth across the supply chain.

In-depth defense within a single actor's SDLC does not positively contribute to the management of shared risk for any other actor. Further, note that defense-in-breadth across the supply chain does not positively contribute to the security of products, solutions, or services created and transported by the supply chain. This situation results from organizations in the cyber supply chain viewing themselves as the terminus in the supply chain rather than a pivot point or orchestrator. This view drives behaviors such as focusing exclusively on supply chain assurance upstream to suppliers and not downstream to customers. Such uni-directional focus effectively prevents an organization's customers and customer's customers from gaining the benefits of an assured supply chain. Recognition of this point is critical when it comes to cyber supply chain management. Because, unlike with many finished goods, cyber systems are procured with a desire to service many classes of customers downstream, often with competing needs, from a singular solution. Such capabilities are available through advanced computing behaviors such as multitasking, cloud computing and grid computing. Recognizing the need to effectively tie together defense in depth and defense-in-breadth in the SDLC and supply chains of nodes and actors within the ecosystem is a great achievement of this framework. The supply chain orchestrator must apply security mitigation strategies to the supply chain and throughout the supply chain [21].

In Figure 7 is the Radar Graphs, the overlapping spans of coverage of five key ICT SCRM initiatives (including the Open Group, ISA and the major three ISO ICT SCRM Standards Development Initiatives) are shown. The initiatives are divided into three levels, namely risk governance, system integration and operation.

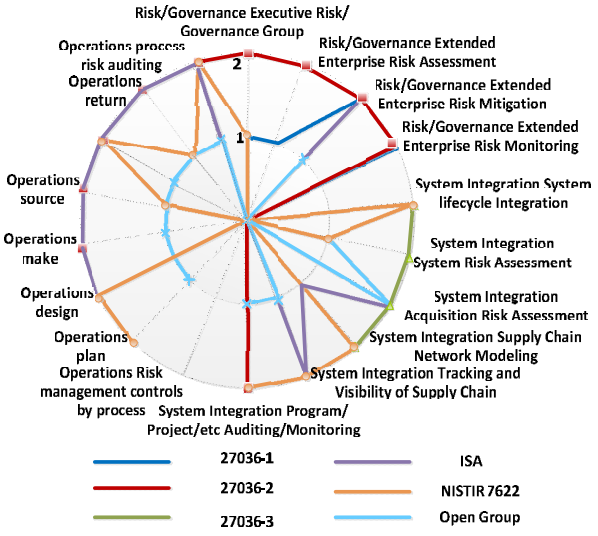

Figure 7. Radar Graphs[21]

The study used a combination of questionnaire, interview and observation to collect data. This was complimented with secondary data from literature. The study used a three scale for responses ranging from no matter taking the value of 0 and being the lower most while strongly recommended was the highest with the value 2. The neutral value had been assigned a value of 1. The investigated organizations or standards ranked their level of initiatives with provided statements on the scale of three (1.No matter 2.Recommended 3. Strongly recommended). We can easily recognize there are still neutrals in the Radar Graphs, which means function with automated business rules and sensor-driven responses are in urgent need in the three-layer ICT SCRM framework.

IV. ICT Supply Chain Case And Suggestions

Here is an instance of the communication equipment supply chain which is typical of ICT products, as shown in Figure 8. If communication equipment manufacturer is the core enterprise, the raw material provider is the initial supplier, the communication material provider is the sub-supplier and the product and the module supplier is the direct supplier. The product and module supplier is separated from the large and comprehensive research and development system of the communication equipment manufacturer. In this way, non-core business or modules with high professional and little correlation to communication can be finished by associated enterprises(Such as audio and video processing modules, many small and medium-sized enterprises can work well in this filed) in the supply chain.

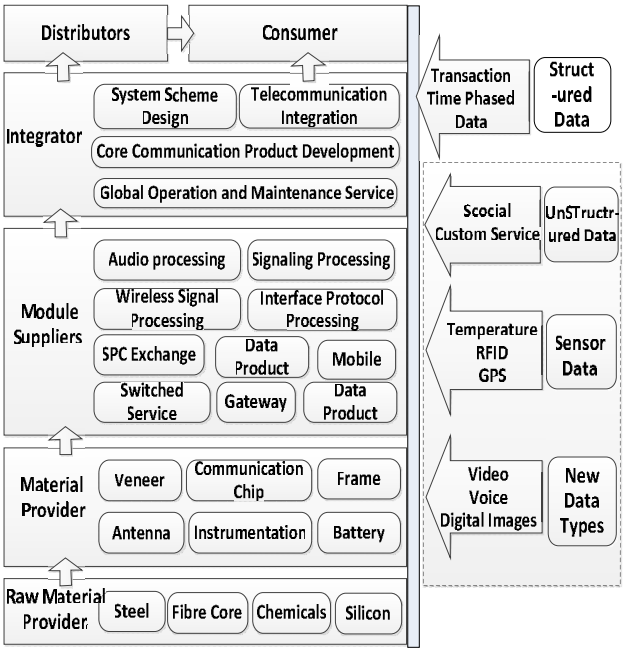

Figure8. Communication equipment with Big Data in supply chain

Based on the five models in the Section III, this paper proposes a series of recommendations conducive to improving security of the communication equipment supply chain from the dimensions of data sharing, integrity, cyber, personnel and risk management.

A. Data sharing

Encrypt data at adequate levels of security; Adopt biometric and other authentication mechanisms for providing data access; Hold time-sensitive data on own servers; Use high assurance routers for more sensitive data; Share worldwide information of high risk shipments between customs and law enforcement authorities; Digital identities given to suppliers to access vendor networks should be controlled with limited access only to relevant resources needed; Each resource shared should have an independent assessments as to the authorization required; Supplier's access to vendor resources should expire as soon as the project completes; A failsafe check should be implemented; A robust procedure using automatic disabling features as well as manual notifications should be used [22].

B. Integrity

Supplier Selection Process: Use a rigorous supplier selection process and a structured qualification program to ensure that only approved suppliers design, develop and manufacture products [23]. Utilize a defined supplier selection process for key suppliers that consists of surveys, onsite audits, sample product evaluations, and pro duct build capability assessments; Administer clearly defined qualification tests prior to engaging in any business with key suppliers; Verify the suppliers' capability to manage and control sub-tier supply chain partners' adherence to specific flow- down requirements; Employ a selection/award process that considers factors other than which supplier has the lowest bid [24].

Contract Requirements& Procurement Practices: Procurement contracts and buying procedures provide significant mitigation against the introduction of counterfeit components. Incorporate specific language in RFIs (Requests for Information), RFQ s (Requests for Quotes), and master purchasing agreements or contracts that drive supplier behavior to help detect and prevent counterfeit components from entering the supply chain; Require suppliers to pass along specific requirements to their suppliers; Require key suppliers to comply with specific standards as appropriate (ISO, TAPA, C-TPAT, etc.); Limit potential exposure to counterfeit parts by making direct dealing with the original manufacturers in purchasing key components [23].

Parts Qualification Procedures: Product qualification procedures should be carried out to ensure that the suppliers adhere to Bill of Material, Approved Vendor List, and product specifications. Provide strict guidance on the specifications and requirements for each component in the pro duct through the Bill of Material. Deviations from the specifications must be approved; Verify that suppliers are in compliance with Approved Vendor List requirements with their sub- tier supplier sourcing [23].

Operations teams should drive strict discipline and governance in manufacturing to provide assurance of supply chain integrity. Use a phase-gate process to manage approvals and drive rigor in every stage of new product introduction; Require continuous monitoring of key process indicators and other critical factory data; Verify unique physical and electronic identifiers on specific components to provide parts trace ability, limiting opportunities for counterfeits to enter the supply chain; Conduct audits regularly to ensure supplier processes are co m pliant with requirements [23].

Secure code: Minimize use of unsafe string and buffer functions; Validate input and output to mitigate common vulnerabilities; Use robust integer operations for dynamic memory allocations and array offsets; Use anti-cross site scripting (xss) libraries; Use canonical data formats; Avoid string concatenation for dynamic sol statements; Eliminate weak cryptography; Use logging and tracing. Vulnerability check: computer based simulations on supply chain security disruptions and vulnerabilities; Determine attack surface and use appropriate testing tools to perform fuzz/robustness testing and penetration testing. Reliable supplier: Give rationalized supply base/focus on trusted suppliers; Enforce e-pedigree/chain of custody documentation and build a simple online record of system-developments in the supply chain [25].

C. Cyber

Network security should be applied using a risk-based process; Session traffic involving source code should be encrypted to acceptable standards; Access to developer workstations should be controlled; Accounts of departing employees should be promptly disabled; Disabled accounts should not be deleted as they can be used for forensic analysis later on; Workstations and virtual machines should be secured to prevent malicious code from being introduced; Developers should have access to the minimum code necessary to complete their task; Tightly enforce "zones of trust" inside network; Integrate digital CCTV with access control logs and LDAP roles/permissions database to monitor network threats; Create a "honey pot": a machine left in a vulnerable state (e.g. unprotected browsers on virtual machines index infections/compromises) and let intruders show their hands; Halt operations if intrusion detection system goes on.

D. Personnel

Ensure all applications are integrated with enterprise LDAP for global identity management; Ensure that application vendors educate internal IT staff on application security best practices; Do pre-production audits of all vendors; Enforce pre-employment screening practices for key personnel; Ensure HR development provides up-to date information to IT department on staff comings and goings to keep LDAPs current; Expand formal credentialing/certifications in secure software lifecycle practices through internal HR or 3rd party trainers; Be alert for disgruntled employees, who can become grave internal threats; Set up risk profiles for job applicants and employees; Make regular interviews with employees and annual police clearance certificate; Make annual supply chain security training for employees; Perform surprise drills for security preparedness; Make duty segregation; Use controlled automated processes; Clearly define roles, responsibilities, and access rights; Management should be aware of who has what access; Train for secure development practices; Train for secure technical controls.

E. Risk management

Build a global visibility grid, a centrally managed "command post" that deploys and monitors digital CCTV and

automated access control lobs across a dispersed network of sites for threat identification and mitigation in real-time; Establish and manage a Risk Registry that captures/defines cyber supply chain priority risks, risk owners, and on-going mitigation actions; Scope chain-wide disruption risks; Prioritize risk for mitigation activities; Assign priority risk to owners and assign resources to risk owners; Create a network map to visualize critical geographically-dispersed cyber supply chain production /distribution /consumption hubs and cyber-nodes; Define command and control/identify supply chain orchestrator to monitor end-to-end flows, handoffs, between actors and total process metrics of effectiveness.

V. CONCLUSION

The use of big data promotes the normal operation of ICT supply chain, which is a carrier of big data in turn. The close relationship between big data and ICT supply chain make it an effective way to do research on big data security though the analysis on ICT supply chain security. As for ICT supply chain, in information networks and information systems, many countries are purchasing foreign IT products and services, which is equivalent to open the door of big data security. So it is necessary to develop the ICT supply chain security measures.

Contemporarily, competition among enterprises is no longer a one-on-one partaking to compete for some terminal market and some customers in a certain time and space conditions, and no longer a traditional way of competition whose main goals is the market share and coverage .While it is a holistic competition across time and space biased on product development and design, raw material purchasing and storage and transportation, product processing and manufacturing, product distribution and delivery, product sales and service and so on. In this new competitive environment, the relationship between core enterprises and their suppliers, distributors, and retailers is no longer the past simple business one, it is the strategic partnership of comprehensive cooperation, benefit sharing and risk pooling, with taking full advantage of big data. Truly successful supply chain requires the concerted efforts of all enterprises in the supply chain. Only every node is safe, can the whole supply chain be successful.

ACKNOWLEDGEMENTS

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; 2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software"; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (NO. CAAC-ITRB-201201).

REFERENCE

[1] Lora Cecere, Founder and CEO, "Go Big or Go Home", Supply Chain Insights LLC, 2012.7

[2] "Serving customers around the corner and around the world", WESCO International, Inc.

[3] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., and Byers, A.H. "Big data: The next frontier for innovation, competition, and productivity",McKinsey Global Institute, 2011

[4] Kevin Orrey, MSc, "A Survey of USB Exploit Mechanisms, profiling Stuxnet and the possible adaptive measures that could have made it more effective",http://www.vulnerabilityassessment.co.uk/education/whitepaper.pdf,2011.4

[5] Steve Wilhelm. Staff Writer, "Boeing 787 battery lags behind evolving lithium-ion technology", Puget Sound Business Journal, 2013.

[6] Comprehensive National Cybersecurity Initiative and United States Naval Institute, "Dealing with today's asymmetric threat, Cyber Threats to National Security", CNCI and USNI, 2010.

[7] Jilin University, Li Quanxi, Zhao Wanchen, "Research on Measurement and Evolutionary Mechanisms of Supply Chain Flexibility", InTechOpen , 2011.

[8] Karine Evrard-Samuel, Université Pierre Mendès-France Grenoble II, France, "Sharing demand signals: a new challenge to improve collaboration within supply chains", 7th International Meeting for Research in Logistics, 2008.

[9] Marianne Swanson, "Piloting Supply Chain Risk Management Practices for Federal Information Systems", Nadya Bartol and Rama Moorthy, 2010

[10] "Software Assurance Forum for Excellence in Code", SAFECode, http://www.safecode.org, last accessed8/31/2009, 2009.

[11] "Priorities for Research on Current and Emerging Network Technologies", European Network And Information Security Agency, 2010.4

[12] "IT SUPPLY CHAIN, National Security-Related Agencies Need to Better Address Risks", United States Government Accountability Office, 2012

[13] CF Chou, "Development of a Comprehensive Supply Chain Performance measurement system: a case study in the grocery retail", master thesis, Massachusetts Institute of Technology, 2004.

[14] Comprehensive National Cybersecurity Initiative and United States Naval Institute, "Cyber Threats to National Security: Countering Challenges to the Global Supply Chain", CNCI and USNI, 2010.8.

[15] LOG 102 Fundamental of System Sustainment Management, "Supply Chain Operational Reference (SCOR) Model Structure".

[16] Husin, Professor John Paul, "Supply Chain Operations Reference-SCOR Model, the Journey to Supply Chain Excellence", 2011.

[17] Robert H.Smith School of business, "Assessing SCRM Capabilities and perspectives of the IT Vendor Community: Toward a cyber-supply chain code of practice", University of Maryland, 2009.

[18] Sandor Boyson, Thomas Corsi and Hart Rossman, "Building A Cyber Supply Chain Assurance Reference Model", Supply Chain Management Center, 2009.

[19] "Transportation&Logistics 2030 Volume 4: Securing the supply chain", Price Waterhouse Coopers, 2011.

[20] "Incorporating Security into the System Development Life Cycle", www.onpointcorp.com/uploads/137/doc/Security_in_the_SDLC.pdf

[21] "The ICT SCRM Community Framework Development Project, final report", The Supply Chain Management Cenrer Robert H. Smith School Of Business University of Maryland College Park, 2011

[22] Rock Automation, "Achieving Secure Remote Access to Plant-Floor Applications and Data", CISCO, 2012.

[23] Jon Amis, Supply Chain Assurance Program Director, "Amis Presentation Dell ANSI-HSSP",2012

[24] Jon Amis, "Anti-Counterfeiting in the Supply Chain", DELL, 2011

[25] Steve Lipner, "Bringing Operational Knowledge to Secure Development", SAFECode and Microsoft Corporation, 2011.