Summary of Discussions at ITU’s Event on
“Combating Counterfeit and Substandard ICT Devices”

**ITU Headquarters, Geneva, Switzerland 17-18 November 2014**

Copies of the [event’s programme](http://www.wto.int/english/news_e/events_e/events_e.htm), [final list of participants](http://www.itu.int/en/ITU-T/C-I/Documents/List%20of%20Participants/Final%20list.pdf) and [contributions](http://www.itu.int/en/ITU-T/C-I/Pages/WSHP-counterfeit-contributions.aspx), as well as other relevant information about the event, are available on the event’s website: <http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx>. A list of acronyms and abbreviations used throughout this Summary of Discussions may be found on the last page of this document.

**Monday, 17 November 2014**

|  |  |
| --- | --- |
|  **14:00 - 14:45**  | **Opening Remarks** |

On behalf of the International Telecommunication Union (ITU), **Mr. Brahima Sanou**, **Director, Telecommunication Development Bureau, ITU**, opened the event with a Welcome Address to participants. Counterfeiting is a growing problem, with a strong negative impact on income, revenues and jobs, while unsafe products present serious health hazards to consumers. He updated participants on the adoption by ITU’s 2014 World Telecommunication Development Conference (WTDC-14), of [Resolution 79](http://www.wto.int/english/news_e/events_e/events_e.htm) on the role of information and communication technologies (ICTs) in combatting and dealing with counterfeit telecommunication devices, and the subsequent adoption by the ITU’s 2014 Plenipotentiary Conference (PP-14) of a [new Resolution](http://www.wto.int/english/news_e/events_e/events_e.htm) on combating counterfeit ICT devices; both of which introduce this issue into ITU’s work programme. Mr. Sanou hoped the event would highlight common concerns, initiatives, opportunities and challenges, as well as a common approach, in the fight against counterfeit products. It is our united responsibility to take steps – Mr. Sanou called on participants to protect consumers.

In his Opening Address, the Chair of the Event, **Dr. Eugene Juwah, Executive Vice-Chairman/CEO of the Nigerian Communications Commission (NCC)**, noted that strong attendance in this event underscores the importance of collective action to curtail counterfeit and substandard ICT devices. Cheaper counterfeit and substandard ICT products are attractive to poor consumers. With the growth and availability of ICT products, counterfeit devices are impacting manufacturers, vendors, operators, consumers and Governments through: loss of revenues, erosion of brand value, loss of goodwill, network disruptions, poor quality of service (QoS) and risks to public health. He cited data estimates of the International Chamber of Commerce (ICC), placing lost tax revenues due to counterfeit goods at US$125 billion for developing countries alone. ICC expects the value of counterfeit goods to exceed US$1.7 trillion globally. The dismantling of barriers and economic integration are inadvertently catalyzing the market for counterfeit and substandard ICT products. Counterfeiters have taken advantage of the strong growth in mobile devices and have circumvented the Equipment Identity Register (EIR), shipping thousands of phones with duplicate International Mobile Equipment Identity (IMEI). He called for concerted global and national effort to combat counterfeiting at national, regional and international levels.

In his Keynote Speech, **Dr. Robert E. Kahn**, **President and CEO, Corporation for National Research Initiatives (CNRI)**, gave his perspectives on combating counterfeit ICT and substandard ICT devices. There is no single turnkey approach that will work for everyone. He described the Digital Object Architecture (DOA) and ITU-T Recommendation X.1255 as a conceptual framework with direct relevance, and the work of the DONA Foundation, a Not-For-Profit (NFP) organization in Geneva, on unique persistent identifiers. He spoke of ICT devices as sources or systems of information (hence their reference as Digital Objects); with each Digital Object having an associated unique persistent identifier – also called a handle – with a resolvable prefix (from the registry, unique to its organization) and a unique suffix. There is a need to manage, update and access information about an ICT device throughout the entire supply chain, either through one or a few interoperable standard mechanism. DOA is one such mechanism that supports resolution of unique persistent identifiers via the Handle System, equivalent to a reliable deployed global Public Key Infrastructure system. The DONA Foundation was set up to oversee the administration of the Handle System and its global handle registry. ICT devices provide various informational components, or handles, which may be either fixed or variable and potentially including: 1) a generic description; 2) relevant details about the software; 3) where the particular device lies in the supply chain; and 4) other information (e.g. store, price, has it been repurposed).

|  |
| --- |
| **14:45-16:30 Policy Debate: Governments’ Perspectives on Combating Counterfeit and Substandard ICT Products** Governments offered their perspectives on their main concerns, challenges and experiences, as well as on their best practices, in combating counterfeit and substandard ICT products. Governments were invited to expand on their perspectives from the legislative, regulatory, customs, law enforcement or judiciary angles.  |

**Mr Lucio COCCIANTELLI**, **Head of Section, Department of the Environment, Transport, Energy and Communications, BAKOM, Switzerland**, moderated the Policy Debate.

**Mr Dmytro PROTSENKO**, **Deputy Director, Radio Service Directorate, the Ukrainian State Centre of Radio Frequencies**, introduced the Automatic Information System for Mobile Terminal Registration in Ukraine (AISMTRU), which was launched by Ukraine on 1 July 2009 to protect the national market from contraband imports of counterfeit and substandard mobile phones. The general structure of the AISMTRU database consists of: 1) white list (legally imported terminals), 2) grey list (terminals with three months to prove their legal origin), and 3) black list (unauthorized terminals not served by telecom networks). The regulator has approved new procedures for imports of radio electronic facilities and radiating devices, as well as for registering international identifiers. He recalled ITU’s WTDC-14 and PP-14 resolutions on the issue of counterfeit ICT devices, and noted that ITU and other stakeholders have key role to play in identifying and coordinating approaches to this challenge. Unique telecommunications/ICT devices’ identifiers may prove helpful, and the creation of a global information system for exchange of unique ICT identifiers may significantly assist Member States. He also gave an overview of initiatives to combat counterfeit mobile devices in a number of countries:

* In Azerbaijan, a database for IMEI codes has been in operation under the Ministry of ICTs since 2013.
* In Colombia, the Ministry of ICT has two IMEI code databases for mobile devices: 1) lost & stolen and 2) legally manufactured or imported.
* In Egypt, the National Telecommunications Regulatory Authority established a Central Equipment Identity Register (CEIR) in 2010 to combat counterfeit handsets. Around 500,000 mobile handsets have been found with fake IMEI codes.
* In India, in 2009, the Government banned services on mobile handsets without IMEI numbers; an estimated 25 million mobile handsets became ineffective.
* In Kenya, the Communications Commission of Kenya gave notice to all mobile network operators to phase out counterfeit handsets from their networks– some 1.89 million counterfeit mobile phones have been phased out since 2012.
* Sri Lanka’s Telecommunications Regulatory Commission intends to implement a National Equipment Identity Register (NEIR) that connects all mobile operators to IMEI databases, and allows network operators to share blacklisted mobiles.
* Turkey’s Communication Technologies Authority established in 2006 a CEIR to prevent the usage of non-registered mobile phones, tax loss, unfair competition, and hijacking. As of the end of 2010, there were some 14 million blacklisted IMEI numbers.
* In Uganda, the Uganda Communications Commission (UCC) has launched a project which aims to gradually eliminate counterfeit phones from the national market.

**Mr Isaac BOATENG**, **Manager, Regulatory Administration, National Communications Authority (NCA), Ghana,** described Ghana’s initiatives. Greater demand for mobile phones has resulted in a rise in counterfeit batteries, accessories and handsets, which can cost as little as $10. Counterfeit mobile devices are very affordable and have contributed to teledensity in the country, while creating youth employment. However, they pose a number of challenges in terms of: health, safety, impact on the environment, Quality of Service, interference and harm to public networks, tax evasion and lack of warranty for consumers. Ghana has a specific problem with e-waste – counterfeit goods break more easily and are creating problems of safe and environmentally-friendly disposal. The company [I](http://www.imeixs.com)meiXS estimates up to 60% of handsets in the market have no IMEI or a replicated IMEI. In March 2014, the [Ghanaian regulator issued ImeiXS a license](http://imeixs.com/news/ghana-regulator-nca-issues-imeixs-a-license-to-operate-an-imei-platform) to implement the GSMA IMEI platform to block counterfeit mobile phones, but the license does not mandate the Mobile Network Operators (MNOs) to connect to this operator to provide effective implementation. The Government has put further requirements in place for imports of mobile phones, namely, tax clearance (from the customs authority) and regulatory clearance for imports, including type-approval certificates. The NCA uses the type approval regime partly to address counterfeiting of ICT devices. Reasons for employing the Type Approval Certificate (TAC) include ensuring that the equipment being imported into the country is genuine, that it meets the minimum technical and regulatory requirements, and that public confidence is boosted. Nevertheless, the NCA is encountering various challenges in the implementation of the TAC, such as dependency on the manufacturers’ own tests results and declaration, lack of independent laboratory verification and market surveillance, existence of porous ports of entry and unapproved routes, and low consumer education on the effects of purchasing counterfeit devices, Ghana initially had a paper-based type approval process, but has now moved to an electronic system, despite some challenges, including a lack of resources. Mr. Boateng recommended that a testing laboratory should be set up for West Africa, and expressed Ghana’s willingness to work with the private sector and other stakeholders. Coordinated global efforts are needed to combat counterfeit and substandard ICT goods, and ITU could take the lead in these.

**Mr Ahmad AL SHAMSI**, **Manager Type Approval, Telecommunications Regulatory Authority (TRA) of the United Arab Emirates (UAE)**, presented the UAE’s experience in how to minimize counterfeit products in UAE. UAE started by defining the problem through looking at the concerns of Government, consumers and industry. The Government aims to protect the telecom sector, the economy, consumers, quality of service and the environment, and it is concerned about loss in revenue. There are also various health, safety, privacy and quality concerns affecting consumers. Many counterfeit devices came with pre-installed apps, which collected data about the consumer. Industry is concerned about their brands, loss of revenues and reputation. The TRA has a clear plan based on three pillars: 1) regulation and enforcement; 2) consumer rights and 3) cooperation with the industry. Under this plan, TRA has:

1. Disconnected fake and duplicate IMEI: on 6 September 2011, TRA issued Directive “Duplicative IMEI” – by 2012, the TRA had disconnected more than 100,000 handsets.
2. Under the TRA awareness campaign, TRA is educating consumers about their rights. Public awareness is still low – people believe that counterfeit devices do the job as well as genuine devices. Raising public awareness, however, is not only a task for the Government, but must be taken in collaboration with the Industry.

Counterfeiters are selling via eBay, as well as exploring different ways of bringing counterfeit devices into a market – e.g. the spare part process, under which counterfeit devices are imported in pieces which are then assembled (including the download of the operating system) and sold.

**Mr Joao ZANON**, **Regulatory Specialist of the Agência Nacional de Telecomunicações (ANATEL) of Brazil**, presented Brazil’s *Sistema Integrado de Gestao de Aparelhos* (SIGA) Project to control counterfeit and substandard ICT devices. Brazilian regulation dictates that operators can allow only authorized devices onto their network. In this sense, multiple sources of information, such as the terminal IMEI and Call Detail Records (CDRs), are processed through the centralized SIGA system to determine if the device is authorized so that operators can take the necessary action to fulfill this regulatory obligation. ANATEL is working with all stakeholders, such as the GSM Association (GSMA), operators and manufacturers to increase the success of the SIGA Project. ANATEL believes that a considerable number of the terminals on the network today are currently unauthorized – this is a very large number and includes different scenarios, such as counterfeit devices, cloned devices, poorly formatted IMEIs or corrupted IMEIs caused by software tampering. Care is needed in approaching each of these scenarios since the consumer impact can be high when blocking millions of devices. In this sense, it may be safer to tackle new terminals. ANATEL is cooperating with customs to try to control the entry of counterfeit and substandard ICT devices at the border. Brazil also has a very strong conformity & interoperability assessment policy that helps on the combat of counterfeit and substandard ICT devices, and has pointed to the importance of making sure that the samples submitted to the conformity tests are representative of what is sold on the market. Brazil also believes it is crucial for the combat of counterfeit and substandard ICT devices to cooperate with international and other organizations such as ITU, the World Intellectual Property Organization (WIPO), the World Trade Organization (WTO), the Inter-American Telecommunication Commission (CITEL), and GSMA. There is a need for multilateral action and raising awareness through best practices and Recommendations, where ITU can be a key player.

**Mr David ROGERS, Mobile Technology, Cybersecurity & Standards, UK Department for Business, Innovation & Skills (BIS)**, emphasized the complex tug-of-war between manufacturers and counterfeiters. He described how counterfeiters may steal authentic labels from old products, polluting databases with outdated authentic information and compromising the database. Countries can invest millions of pounds in anti-counterfeiting systems, but they may become redundant quickly. Creating global, centralized kill mechanisms not only risks creating centralized points of failure vulnerable to cyber-attacks, but also raises consumer privacy concerns. Legal equipment could be re-marked as counterfeit and disabled, in case of war. The UK has a strong multi-agency response, but the number of counterfeit devices is increasing. Some countries have been identified as the source manufacturers of counterfeit ICT devices, and their Governments need to deal with this problem, otherwise other countries are dealing with symptoms, not the root causes. We need to acknowledge we are all part of the solution, and we all need to work together. No single body can deal with this issue. We need to deal with the criminals involved, while respecting the privacy of end-users.

|  |
| --- |
| **17:00-19:00 Intergovernmental Initiatives Against Counterfeit and Substandard ICT Products**This session presented key international legal frameworks and intergovernmental programmes/initiatives that have been established by intergovernmental organizations (IGOs) to protect and enforce intellectual property rights (IPRs) or to combat counterfeit and substandard ICT products. These IGO initiatives highlighted their main challenges and notable experiences in the fight against counterfeit and substandard ICT products. Potential key areas for future cooperation, coordination and improvement were also identified.  |

**Ms Marie-Elisabeth D'ORNANO**, **Chairwoman, International Electrotechnical Commission Quality Assessment System for Electronic Components (IECQ)**, moderated this session and introduced the panelists.

**Ms Louise VAN GREUNEN**, **Director of the Building Respect for IP Division at the World Intellectual Property Organization (WIPO)**, described WIPO’s work in intellectual property (IP) enforcement. She underlined the need to be clear on definitions – for WIPO and WTO, counterfeiting relates to a subset of infringement of trademarks. A substandard product may be non-compliant vis-à-vis regulatory standards, but it may have a national trademark, in which case it would not be counterfeit. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) gives guidance about what constitutes counterfeit goods. TRIPS creates an obligation on Member States to make criminal penalties available for willful trademark counterfeiting on a commercial scale. However, there is public demand for, as well as availability of, these illegal goods; it is difficult to change consumer behavior unless consumers understand these goods can damage their health and safety. Ms. Van Greunen touched upon the work of the WIPO Advisory Committee on Enforcement, whose mandate includes working with other stakeholders to combat counterfeit goods, including through cooperation, coordination and awareness raising. She also called for improved methodologies and reliable statistics to get a better picture of the scope of the problem, its causes and its socio-economic impact. WIPO is involved in the [Global Congress on Combating Counterfeiting and Privacy](http://www.ccapcongress.net). WIPO’s Patent Landscape Report on ‘E-Waste Recycling Technologies’ refers to ICT/telecom devices.

**Mr Jean BERGEVIN**, **Head of Fight Against Counterfeiting and Piracy Unit, Intellectual Property Directorate, European Commission (EC),** presented a recent ten-point action plan from the European Union on “IP-infringing products”, which are not just counterfeit goods – it is vital to be clear what is under discussion. He noted the need for:

1) A holistic and inclusive approach involving regulators, Governments, consumers, the industry.

2) Focusing on prevention, and killing the incentives early across the whole supply chain.

3) Assistance working with the different actors.

Supply chains are increasingly following conformity and assessment procedures, including track-and-trace technologies (the aviation industry is the most advanced here). Within the ICT industry, mobile phones are clearly the largest source of concern when it comes to counterfeiting and substandard practices, but counterfeit and substandard ICT accessories, chips and other components also now infiltrate the supply chain. Many counterfeit ICT products now make it into military defense equipment; construction (e.g. 10% of circuit-break switches catch fire); and medical devices. Online provision is a ripe source for counterfeiters. He concluded that there is no silver bullet solution, but highlighted that the European Commission’s services would be pursuing the following four steps in developing its thinking on this issue: 1) consultation and exchange of views among EU public authorities through the IPR enforcement expert group it had recently established; 2) a report to be prepared by the Joint Research Center at the European Commission to gauge the scope of the problem and map existing best practices in responsible supply chain management; 3) a thematic workshop with a broad range of stakeholders that would review the report to determine best practice and assess the need for policy orientation; and 4) a major public conference at which a Commission Communication setting out potential policy options could be launched. Mr. Bergevin hoped that this could be undertaken and completed by the end of 2015, subject to agreement within the new Commission. He also noted that issues of privacy and consumer rights are key – mobile phone users can’t just be cut off the network. The criminals really are operating within the European single market and internationally. They are the best at crossing borders with ease and moving around to avoid restrictions and tax. The ex-post application of regulation to seek redress therefore does not work alone– a preventative approach is needed to tackle the problem at its source.

**Mr Roger KAMPF, Counsellor, IP Division of the World Trade Organization (WTO),** pointed out that the WTO’s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) was the first international treaty that provided for a comprehensive set of rules regarding the enforcement of IPRs. He called for greater clarity in definitions and terminology:

* counterfeit (a trademark issue; infringement of a trademark with intent to deceive consumers);
* infringement of trademarks (may confuse consumers, but lacks malicious intent to deceive);
* contraband equipment (a trade issue; infringement of customs regulations); and
* substandard equipment (a regulatory issue).

These are all separate terms, which should not be used interchangeably. He cited some examples where terminology had confused either the analysis or the response, and cautioned against linking the issue of counterfeiting to patents (as opposed to trademarks) in order to avoid broadening the meaning of counterfeiting. The terms and scenario also shape the response, as TRIPS, for example, can help to fight counterfeit ICT goods – but not to combat substandard ICT equipment (as this is a regulatory issue, not related to IPR). Of the 245 Regional Trade Agreements that had been notified to the WTO by February 2014, depending on when these agreements entered into force, between 40-70% have provisions on cooperation, customs and enforcement. As part of the way forward, there may be a need 1) to foster cooperation and collaboration among all stakeholders; 2) to raise awareness and build capacity at all levels, and 3) to gather more facts and empirical data about the real nature and impact of counterfeit goods because the assumption, for example, that counterfeit phones are necessarily of poor quality and bad for health needs to be backed by solid data.

**Mr Piotr STRYSZOWSKI**, **Economist, Directorate for Science Technology and Industry of the Organisation for Economic Cooperation and Development (OECD)**, began by announcing that OECD will conduct a new study in the area of counterfeit and pirated trade, aiming to: assess the magnitude of problem by gathering additional empirical data; study its potential economic effects (in terms of, for example: employment, profit and growth); and make relevant policy conclusions. Going back to the OECD’s 2008 study on the same subjects, he highlighted that measurement in this area is difficult due to very limited data availability. Consequently, the OECD methodology actually looks at tangible products that infringe trademarks, copyrights and design rights based on surveys from customs authorities, which are extrapolated through the World Customs Organization (WCO). In terms of key messages – everything can be counterfeit, including luxury goods, pharmaceuticals, cosmetics, food, toys, ICT devices, clothes, etc. This is a horizontal problem, affecting multiple sectors. A reinforced policy, legal regulatory framework is needed across multiple sectors, including cooperation among different ministries and governmental authorities, IGOs and industry, and with a strong emphasis on enforcement. Raising awareness and consumer education is vital, but this is important not only end users, but also for businesses and government officials. The OECD will update its figures with latest data next year.

**Ms Samantha GOMPEL**, **Communications Manager, IPR and Health & Safety Programme, World Customs Organization (WCO),** introduced the work of WCO based in Brussels, with 179 Member States. WCO aims to harmonize customs procedures and facilitate trade. Counterfeiting is not necessarily a priority – each country sets its own priorities; for some of countries, seizing the importation of narcotics, firearms or endangered species at the border is a higher priority than seizing counterfeit or illicit products. Approximately 1.1 billion products were stopped as part of Operation Biyela in Africa, of which 40% were electronic appliances, which can be extremely dangerous/hazardous to consumers. WCO delivers capacity building programmes, including: operations; diagnostics; seminars; identification training; and IPM, a database with information on what counterfeit products look like, packaging, routes of shipping and transit, previous cases and contact information. WCO publishes an annual illicit trade report. Ms. Gompel concluded that there is a strong need for cooperation.

|  |
| --- |
| **Tuesday, 18 November 2014** |

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
| **09:00-10:45**  |

 | **Technology Debate, Part 1: ICT industry perspectives and anti-counterfeit/substandard technologies and systems**  |
| This session 3.1, as well as session 3.2 below, explored various types of technologies and other technical measures used by governments and rights’ holders in combating counterfeit and substandard ICT products. In particular, ICT industry players highlighted their respective concerns, main challenges, best practices and notable experiences in their fight against counterfeit and substandard ICT products.  |

**Moderator: Mr Felipe BATISTA**, **Secretary, Associação de Reguladores de Comunicações e Telecomunicações da Comunidade dos Países de Língua Portuguesa** (**ARCTEL-CPLP),** moderated this Session. He stated that this is a very important topic for ARCTEL – a regulatory association which gathers eight Portuguese-speaking countries in four different regions of the world, affected strongly by counterfeiting. ARCTEL brought this topic forward in 2012 at ITU’s Global Symposium for Regulators (GSR), and believes this topic must be tackled by all stakeholders to find common paths.

**Mr Thomas BARMUELLER, Director, EMEA, Mobile Manufacturers Forum (MMF),** introduced MMF as representing the vast majority of global handset sales and the majority of global handset infrastructure. MMF is active in research and standards support, regulatory harmonization and public communications. In 2011, 125 million substandard and counterfeit handsets were sold globally, which increased to 148 million in 2013. Counterfeit mobile phones have negative implications on consumer privacy; with many of them having imbedded spyware targeting consumers’ personal and financial data. Counterfeit and substandard mobile devices also pose growing threats to consumer health and safety, as they are not tested for compliance and contain dangerously high levels of lead and cadmium in phone parts exposed to consumers. As seventy percent (70%) of consumers wrongly believe counterfeit devices were of the same high quality as genuine phones, raising consumer awareness remains important, such as through MMF’s “Spot a Fake Phone” campaign. MMF cited research related to counterfeit phones and network performance – counterfeit phones drop 1 in 4 calls, delay handover and even fail in every third handover. While in the past network coverage was of utmost importance, stakes have changed due to the focus of regulators on Quality of Service (QoS) in congested networks. Operators can tackle and reduce the number of counterfeit phones operating on their networks in order to increase QoS. There is a need for a national action plan – increasing consumer awareness and enforcement, identifying best practices in regulatory activities, and collaborating among all stakeholders are all very important parts. One may not have to change the legal environment, but simply use what is in hand and increase enforcement – this is not an argument against introducing new legislation, but a call to make the best of what is in place already.

**Mr James MORAN, Security Director, GSM Association (GSMA),** described the work of the GSMA and its International Mobile Equipment Identifier (IMEI) database. The GSMA, a trade association representing the interests of mobile operators, maintains the IMEI as a globally recognized, universally applicable system to uniquely identify mobile phones. GSMA has been the global designator and the only source of IMEI since 2004. The IMEI is a 15 digit code, of which the first eight digits is the Type Allocation Code (TAC) issued to equipment manufacturers. The database is controlled, centrally stored, and confidential, and structured to facilitate search and storage. GSMA is responsible for keeping the data confidential, and for making them available to everyone eligible. Over 700 mobile operators, 14 national regulatory and law enforcement agencies, and 2 customs agencies have used these data to recover devices, prevent device laundering, and enhance consumer protection. GSMA also has enforcement responsibilities and a dispute resolution mechanism. There is a need to continue to invest in IMEI and security – GSMA is willing to support all efforts to combat counterfeit, and encourages all stakeholders to use its data. GSMA is willing to work with all stakeholders to build the ecosystem and preserve the use and importance of the IMEI.

**Mr. Kah-Kin HO, Head of Strategic Security Corporate Technology Group, Cisco Systems,** presented Cisco Systems’ cradle to the grave approach to security throughout the supply chain in machine to machine and the ‘Internet of Everything’. When designing a product, security must be taken into account from the start – security cannot be bolted on later – it must be built in from ideation of the technology, through quality control, logistics, supply of solutions to end-of-life disposal. Cisco is unable to solve this problem alone, and works closely with suppliers, logistics partners, customs officers, enforcement. There are three ***major threats*** to customer trust in Cisco (*1) manipulations; 2) espionage; and 3)* *disruption*), which give rise to three ***exposures***: 1) *Taint* (unauthorized automation of a product for espionage and developing control); 2) *counterfeit* (in raw materials, components, and finished goods) and 3) *IP misuse*. To combat these exposures, Cisco uses a combination of security technology, physical management and logistics security:

* Cisco has anti-counterfeit chips to detect breaches.
* Cisco has a trust anchor technology programme, where hardware and software are verified to be authentic.
* Every component can be traced to finished goods, with real-time tracking of where goods are.
* Logistics security includes role-based access control, encryption to suppliers and other things.

Proliferation of new standards is not helpful – existing standards should be reviewed and harmonized.

**Mr Peter FIFKA, Senior Programme Manager for Investigations, from Digital Crimes Unit at Microsoft,** presented Microsoft’s work. Microsoft has a group of almost one hundred professionals (attorneys, investigators, analysts and technical experts) located around the world working on different topics relating to counterfeiting, piracy and cyber-security, including: malware disruption; IP protection; and protection of vulnerable populations. Engineering can help make products more difficult to copy, but follow up in enforcement is also necessary. Microsoft sees existing legal frameworks as sufficient, but they need to be fully utilized – its legal team is applying various innovative strategies and legal instruments to further strengthen the security of IT networks running on its technology. Microsoft is relatively a newcomer to mobile devices, following its acquisition of Nokia’s Devices and Services business, but is using its experience from years of combating software counterfeiting. Microsoft has recently carried out research into counterfeit and refurbished (original) phones – mainly into Windows phones, but others as well—by purchasing these mobile devices in China and elsewhere in order to better understand: 1) how they replicate original features, 2) whether they are infected with any malware, and 3) whether they present any health or safety concerns, or any differences in performance. The prices of these counterfeit phones were higher than expected, and it was found that 7 of 16 phones were infected with malware. This analysis found some basic problems, but also some dangerous threats – pirating personal information from the mobile phone or making payments from the phone. The link between malware and counterfeit devices is similar to the experience of software in the past – the first stage is to make cheap replicas, sell them and make money. Now, counterfeiters aim also to access the users’ data and control the device.

**Mr George WIESSING, Security Investigations Manager of Hewlett Packard (HP),** presented trends in different types of ICT and printing equipment being counterfeited, and noted the health and safety risks posed by such equipment. The issue is not only limited to printing supplies, but also extends to ICT components and accessories such as laptops, adapters, batteries, servers, hard drives, and even USB flash drives. He also described HP’s Global Anti-Counterfeit Program (ACF) comprised of five pillars:

1. Prevention and education – internal and external (law enforcement and customs officials) through e-learning modules and by hosting and attending events.
2. Channel management – ensuring the channel can deal with risks and securing supply chains.
3. Investigation and enforcement –strong focus on removing counterfeit goods from market.
4. Product and packaging – it is vital to improve/distinguish one’s genuine product/packaging from that of counterfeiters, and to use sophisticated security labels that are difficult to replicate.
5. Government relations and legal – HP is very active here with legislators in general.

Only 6% of corporate customers who purchased counterfeits did so intentionally according to a survey carried out for HP in July 2013. For HP printers, if counterfeit cartridges are used, the printer will inform the end-user, and there are options for consumers to report the issue to HP, so HP can follow up. For printing supplies and hardware products, HP has introduced various types of security labels (e.g., holograms). Ink and toner security labels have a QR code which can be scanned using an HP mobile application, thereby allowing the end-user to authenticate a product prior to purchase. The program has continuous success in seizing large quantities (i.e., tens of thousands) of counterfeit HP goods, for example in China, Saudi Arabia, Africa and Western Europe.

|  |  |
| --- | --- |
| **10:45-11:15**  | **Coffee Break**  |

|  |  |
| --- | --- |
| **11.15 – 13.00** | **Technology Debate, Part 2: ICT industry perspectives and anti-counterfeit/substandard technologies and systems**  |

**Mr Glenn JONES, Steering Committee Member, Business Action to Stop Counterfeiting and Piracy (BASCAP), International Chamber of Commerce (ICC)** and Hewlett-Packard Global Anti-Counterfeit Programme, moderated this Session. He introduced the work of BASCAP, an initiative that actively lobbies Governments and non-governmental international organizations in relation to counterfeiting issues, and which is comprised of 24 companies including HP. BASCAP has estimated that the total global economic value of counterfeit and pirated goods will soon reach US$1.77 trillion. Counterfeit is not just fake luxury goods – but also ICT products and counterfeit medicine (i.e., the World Health Organization estimates that 10-30% of drugs are counterfeit). Factors driving organized crime’s entry into IP crime include: 1) Profit versus risk; 2) Modest legal penalties; and 3) Often lax enforcement of IP crime.

**Mr Zhou JIAN, Director, Informatization Research and Promotion Center of the Electronic Technology Information Research Institute under the Ministry of Industry & Information Technology of China (MIIT China),** presented China’s work in this area, with a focus on the food industry and its quality, and the use of IT to enhance the food safety. Quality is a critical issue for the food industry, as demonstrated by the case of melamine in Chinese baby milk and the resulting crisis in consumer confidence this product. He stated that control assurance mechanisms must focus on prevention, inspection and quick response, and noted that raw materials must also be the subject of quality compliance. Mr. Jian called for a credible public traceability system under which all enterprises in the supply chain can serve as data sources for traceability. China has introduced the handle system and Digital Object Architecture (DOA) as its core technology for food quality traceability. Handles are flexible, extensible and compatible with the products and can help solve security problems. The handle system has helped: 1) consumers by making it easy and convenient to obtain information, thereby boosting confidence and raising credibility; 2) enterprises by avoiding duplication of efforts and reducing investing; and 3) governments by facilitating supervision, regulation and enforcement. Standardization is necessary for enterprises to acquire the platform service. Today, six large Chinese baby food enterprises are using this system, and there were 80 million registered handles in use by October 2014.

**Mr Martin BERNHARDT, Vice President, Relations with International Institutions, Sanofi, International Federation of Pharmaceutical Manufacturers & Associations (IFPMA),** described the main issues in relation to counterfeit medicines and pharmaceutical products. He made a clear distinction between counterfeit and substandard medicines, which are not the same. Medicine which is legally manufactured and approved, but which does not meet all of the required quality criteria, is substandard and may pose health risks; while counterfeit medicine is one which is deliberately and fraudulently mislabeled and is a crime against patients. Counterfeit medicine traffic is growing every year, and is now a real public health threat as well as a very profitable crime. At least 10% of all medicine is fake, up to 50% online on illegal internet sites, while in developing economies, 10-30% of drugs are counterfeit. Revenues from counterfeit medicines are as high as US$75-$200 billion per year. Return on Investment (RoI) is high – for $1 invested in narcotics, RoI is $100; while RoI may reach $1,000 in counterfeit medicine. Counterfeit medicines pose global public health risks (including resistance to treatment, disability and death) and undermine trust in health systems, while everyone is affected – patients, Governments, health professionals and manufacturers. Precisely because counterfeit medicines are a multistakeholder issue, there is a need cooperation among Governments, law enforcement agencies, regulators, IGOs, non-governmental organizations (NGOs), industry and other relevant partners in order to raise awareness and craft a holistic approach that tackles the problem at its source. There is no single technological solution to fight against this problem, but there should be a tight control throughout the supply chain, at least. Track & Trace systems help, but the cost of their implementation is high. Pilots using m-Technologies are in place in Africa and give promising results. In order to reinforce awareness on the risk of counterfeit medicines, IFPMA and more than 25 key partners have joined forces to create the “Fight the Fake” campaign. On the enforcement side, Interpol plays a key role. It is essential to reinforce the regulatory and legislative frameworks, at the national or regional level, and also to reinforce the WHO leadership on the fight against counterfeit medicines.

**Mr Yves JOBIN, Business Development Manager from Société Générale de Surveillance (SGS) and Mr Olivier POULAIN, Program Manager, CME Mobile Device Management at Hewlett-Packard (HP)** gave a joint presentation. Mr. Jobin gave an overview of the work of SGS, which provides services to a variety of industries including the telecommunications sector. There are two SGS solutions in place to combat counterfeit and substandard communications devices: 1) its Product Conformity Assessment (PCA), and 2) its Central Equipment Identity Registry (CEIR). Under the PCA, SGS works with customs authorities to inspect, verify, test, assess and certify the conformity of products based on the requirements of the importing country. Product conformity assessments and certifications are carried out through laboratory results, manufacturing audits and physical inspection taking place prior to the time of importation, thereby expediting the customs clearance process. Requirements are evolving and SGS is increasingly focused on supplier protection, C&I. If counterfeit or substandard goods are blocked at customs, experiences show that they may nevertheless filter into the country via other channels. To challenge counterfeit, there is a need to verify, survey and enforce – verification is an important aim of the SGS PCA scheme, just as surveillance is an important aim of the SGS CEIR scheme. Mobile devices are high-value, limited volume devices, which can enter a country out of the regular trade process, or are subject to theft. Mr. Jobin presented the Central Equipment Identity Register solution (with reference to a deployment in Tanzania using HP technology) as a tool to fight counterfeit and substandard ICT devices. The CEIR solution can monitor—in real time—the subscriber and device population based on Subscriber Identity (IMSI & MSISDN) and device identity (IMEI) for identifying and blocking, if need be, counterfeit devices. For this, the CEIR solution can connect to the GSMA IMEI database or other industry source of data that can be useful to cross reference the device’s identities. However, there is no single approach that will give a complete solution for counterfeit or substandard ICT goods. Difficulties in coordination can arise – the PCA scheme is usually managed by the Ministry of Trade, while CEIR is managed with the Ministry of Telecommunications; and governmental entities need therefore to cooperate within countries.

**Mr Keith MAINWARING, International Projects Consultant, Ukrainian National Information Systems (UNIS),** gave an overview of the forthcoming ITU-T Study Group 11’s Technical Report on Counterfeit and Substandard ICT products, and described the main subjects covered by the report.

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
| **14:30-16:30**  |

 | **Interactive Dialogues on the Way Forward ITU: Development Opportunities and International Standards as part of the Global Strategy against Counterfeit and Substandard ICT Products** |
| This session featured a series of interactive, collaborative dialogues among all participants concerning the roles and activities that ITU could take as part of the global strategy to fight counterfeit and substandard ICT products. Within such context, this session aimed to identify specific actions to be taken by ITU in order to develop technical tools, facilitate the gathering and exchange of knowledge, information and practices, raise awareness, and increase coordination and collaboration among the various stakeholders. **Moderator: Mr Tomas LAMANAUSKAS**, Head, Corporate Strategy Division, ITU.**Rapporteurs: Mr Joao ZANON**, Regulatory Specialist of the Agência Nacional de Telecomunicações (ANATEL) of Brazil; and **Mr Keith MAINWARING**, International Projects Consultant, Ukrainian National Information Systems (UNIS).**Methodology of Interactive Dialogue Series:** This session was divided into 2 conversation rounds each guided by a question, as follows: • How effective are current initiatives to combat counterfeit and substandard ICT devices proving sufficient, and how can they be better improved?• What is the role for ITU in combatting ICT devices?At the end of each round, all views and ideas issuing from the conversation were collected and shared with all participants. Additionally, two brief town-hall sessions were held in order to identify the overall trends, collective insights, common solutions or follow-up actions generated by the group at large. |

In response to Question 1, participants were relatively united on the fact that the problem is growing, despite the best efforts to combat counterfeit and substandard ICT devices. Participants agreed that there is a need to improve customer centricity, to tackle the criminals and to get to the underlying source of the problem. Participants noted the importance of cost versus benefits approach – it would be possible to track, trace and tag many products, but the costs could vastly exceed the benefits. There is a need to align interests better – the counterfeiting problem affects stakeholders to different extents – for example, operators may not actually care very much about counterfeit goods, as long as counterfeit handsets or chips do not impact network performance or traffic over their network.

With regards to Question 2 on ITU’s potential role in relation to combatting counterfeit goods, there is a need to increase awareness, capacity-building and collaboration, including through best practices. In one extreme, some people have suggested a global database, while at the other end, there are opposing views. Consensus falls in the middle, where people are suggesting best practices and guidelines and capacity-building by ITU, where ITU has a proven track record. ITU should also work with the external agencies, WCO, WIPO, WTO and so on. The ITU could coordinate effectively with other global bodies (e.g. WIPO, WTO) to forge a global fight. ITU could also act as a convener, bridging policy-makers and industry, for example.

|  |  |
| --- | --- |
| **16:30-17:00**  | **Closing**  |

|  |
| --- |
|  |

In light of Dr. Eugene Juwah’s return to Nigeria for professional reasons soon after the opening of the event, Dr. Juwah delegated his role as Chairman of the event to **Mr Isaac BOATENG**, **Manager, Regulatory Administration, National Communications Authority (NCA), Ghana**. As Chairman, Mr. Boateng delivered his Closing Remarks summarizing trends and key points that emerged during the event. The event’s discussions centered around three trends: (1) the scope of the problems raised by counterfeit and substandard ICT devices; (2) the negative impact of counterfeit and substandard ICT devices on the various stakeholders; and (3) the actions that ITU can take to combat counterfeit and substandard practices.

Under the first trend, the event highlighted the need to distinguish between “counterfeit” versus “substandard” products. Whether an ICT device is “counterfeit” is determined in relation to its trademark infringement under national law. A counterfeit product is one that, without permission, bears a trademark that is identical or indistinguishable from a registered trademark for that product under the laws of the importing country, with the intent to defraud and give the impression of authenticity. Whether an ICT device is “substandard” is determined in relation to its non-compliance with national and international technical standards, conformance & interoperability assessments, or legislative or regulatory requirements. As a result, it is possible for an ICT device to be counterfeit but not substandard, and vice versa. One should avoid using interchangeably the terms “counterfeit,” “substandard,” “contraband,” “illegal” or “unauthorized”; as they are not the same thing. Mr. Boateng also observed consensus that counterfeiting and substandard issues affect not only the whole ICT industry, but also other industries such as pharma, transportation and food. Within the ICT industry, the effects of counterfeit and substandard practices extend beyond mobile phones to other ICT products (such as tablets, personal computers, digital cameras and medical equipment), accessories and components. ICTs are an essential tool to combat counterfeiting of ICT devices and products in other industries.

Under the second trend, the event explored the negative impacts of counterfeit and substandard ICT devices on governments, businesses and consumers. For governments, the proliferation of counterfeit and substandard ICT devices translates into (1) loss of revenues, customs duties and taxes, and (2) impediments to protection of businesses, consumers and the ICT industry by undermining the enforcement and effectiveness of various laws, regulations and programs. For industry, counterfeit and substandard ICT devices mean (1) lost revenues, (2) dilution of their trademark value, and (3) loss of consumer trust. Consumers also suffer negative consequences from substandard ICT devices, including: (1) poor performance, (2) low QoS, (3) privacy and security concerns, and (4) threats to health and safety.

The third trend showed consensus about the main building blocks of a holistic anti-counterfeiting strategy. Mr. Boateng noted that, in fulfilling its mandate under WTDC-14 Resolution 79 and the new PP-14 Resolution, ITU’s role in combatting counterfeit and substandard ICT devices could also be centered around these main building blocks, namely:

(1) Multi-stakeholder cooperation—ITU could leverage its public-private membership and relations with other organizations to foster cooperation in the area of counterfeiting;

(2) Gathering and sharing of information—ITU could facilitate the collection, analysis and exchange of information about counterfeiting and substandard practices in the ICT sector, and about how ICTs could be used in the ICT/other industries as a fighting tool;

(3) Building capacity and raising awareness—ITU could raise awareness among stakeholders about the negative effects of counterfeit and substandard ICT devices;

(4) Use of technical solutions – ITU could continue the discussion on the role of IGOs in using technical standards and conformance & interoperability programs to combat counterfeit and substandard ICT devices; and

(5)  Development and enforcement of adequate legal, regulatory and policy measures—ITU could assist Member States in doing this; such measures should be comprehensive, effective and custom-tailored, yet consistent with best practices at the regional and international levels.

In his Closing Remarks, **Mr Malcolm JOHNSON, Director, Telecommunication Standardization Bureau, ITU,** thanked everyone for attending, and noted ITU’s willingness to work and collaborate with all stakeholders on important issues in ICT, such as counterfeit and substandard ICT devices. ITU will be in touch again soon with recommended actions from the event. ITU will also reflect on how to implement some of these proposals, based on the clear mandate merging from WTDC-14 and PP-14. ITU’s membership has clearly endorsed ITU to take this work forward, as a major concern in many of ITU’s Member States, and ITU will do this in partnership with the stakeholders, so as to minimize duplication of efforts.

**LIST OF ACRONYMS AND ABBREVIATIONS**

ACF Anti-Counterfeiting program of Hewlett Packard

ANATEL Agência Nacional de Telecomunicações (of Brazil)

AISMTRU Automatic Information System for Mobile Terminal Registration in Ukraine

ARCTEL-CPLP Associação de Reguladores de Comunicações e Telecomunicações da Comunidade dos Países de Língua Portuguesa

BASCAP Business Action to Stop Counterfeiting and Piracy

BIS Business, Innovation & Skills Department of the United Kingdom

CAK Communications Authority of Kenya (formerly the Communications Commission of Kenya)

CEO Chief Executive Officer

CEIR Central Equipment Identity Registry

CNRI Corporation for National Research Initiatives

DOA Digital Object Architecture

EIR Equipment Identity Register

GMSA GSM Association

HP Hewlett-Packard

IECQ International Electrotechnical Commission Quality Assessment System for Electronic Components

ICC International Chamber of Commerce

ICT Information and Communications Technology

IFPMA International Federation of Pharmaceutical Manufacturers & Associations

IGO Intergovernmental Organization

IMEI International Mobile Equipment Identifier

IMSI International Mobile Subscriber Identity

IP Intellectual Property

IPRs Intellectual Property Rights

ITU International Telecommunication Union

MIIT Ministry of Industry & Information Technology (of China)

MMF Mobile Manufacturers Forum

NCA National Communications Authority (of Ghana)

NCC Nigerian Communications Commission

NGO Non-Governmental Organization

OECD Organisation for Economic Cooperation and Development

PCA Product Conformity Assessment

PP ITU’s Plenipotentiary Conference

QoS Quality of Service

RoI Return on Investment

SIGA Sistema Integrado de Gestao de Aparelhos

SGS Société Générale de Surveillance

TAC Type Allocation Code or Type Approval Certificate

TRA Telecommunications Regulatory Authority (of the United Arab Emirates)

TRIPS Agreement on Trade-Related Aspects of Intellectual Property Rights

UCC Uganda Communications Commission

UNIS Ukrainian National Information Systems

WCO World Customs Organization

WIPO World Intellectual Property Organization

WTDC ITU’s World Telecommunication Development Conference

WTO World Trade Organization