http://www.rasi.vr.uff.br
RASI, Volta Redonda/RJ, v. 6, n. 1, pp. xx-xx, jan./abr. 2020.

Internet da Coisas a serviço da Defesa: proposição de um sistema de rastreamento de armamentos.

Tarso de Souza Ramalho (POLI- USP) tarso@hotmail.com
Marcos Cesar Weiss (FEI) mw@marcosweiss.com.br
Vidal Augusto Zapparoli Castro Melo (POLI-USP) vidal_melo@pea.usp.br
Sergio Takeo Kofuji (POLI-USP) kofuji@usp.br

RESUMO:
Esse trabalho tem por objetivo propor um sistema de rastreamento de armamentos. Para atingir o objetivo, optou-se por uma abordagem metodológica de caráter qualitativo com dados secundários coletados por meio de pesquisas bibliográfica referentes à armamentos de uso policial e das Forças Armadas, bem como sobre o uso de tecnologias de Internet das Coisas (IoT) e Sistema de Identificação por Radiofrequência (RFID) para esse tipo de aplicação. As análises foram realizadas com base na correlação da literatura encontrada com a proposta do estudo de se viabilizar o rastreamento de armamentos por meio das tecnologias apresentadas. O controle se inicia na fabricação, quando é embarcado o *tag* no armamento para permitir seu monitoramento desde sua fabricação e durante sua utilização. Em caso de qualquer tipo de adulteração, o armamento é danificado e fica com sua usabilidade comprometida. A proposta aborda, também, a integração com os sistemas atualmente utilizados no Brasil – SIGMA e SINARM – e passem a contar com dados mais consistentes, além de incrementar a eficiência no controle de movimentação do armamento tanto em ambientes controlados quanto em ambientes públicos. A contribuição é diretamente relacionada com a proposição de uma solução para rastreabilidade de armamentos e indiretamente com a geração de inovações que visem a redução da violência.
PALAVRAS-CHAVE: Internet das Coisas. Rastreabilidade. Armamentos. Sensores RFID.

Internet of Things at the service of the Defense: a proposition of a weapons tracking system.

ABSTRACT:
This paper aims to propose a weapon tracking system. In order to achieve this objective, a bibliographical research was carried out regarding weapons used by the Police and Army Forces, as well as the use of Internet of Things (IoT) and Radio Frequency Identification (RFID) for this type of application. The analysis was carried out based on the correlation of the literature with the proposal of tracking weapons through based on the presented technologies. The control begins inside the manufacture, where the tag is installed in the weapon and allow its monitoring throughout the utilization. In case of any type of tampering, the weapon can be damaged and with the usability compromised. The proposal also addresses the interoperability with legacy systems currently in use in Brazil - SIGMA and SINARM – in order to rely on more consistent data, as well as increase efficiency to control the shipping of weapons in controlled and public environments. The study directly aims to contribute for a solution for the traceability of weapons and indirectly to the generation of innovations to reduce violence.
KEYWORDS: Internet of Things. Traceability, Weapons. RFID Sensors.

Universidade Federal Fluminense
R. Desembargador Ellis Hermydio Figueira, 783, Bloco A, sl. 218, Aterrado.
27213-415 - Volta Redonda, RJ – Brasil
www.uff.br

Recebido em 11/01/2019
Aceito em 08/07/2019

10.20401/rasi.5.3.41

Avaliado pelo sistema double blind review
Editor: Marcelo G. Amaral

Internet da Coisas a serviço da Defesa: proposição de um sistema de rastreamento de armamentos.

1. Introdução

A inovação tem sido nesse início de século XXI a mola propulsora para que avanços em processos e produtos possam imprimir melhores capacidades de resolução de problemas das organizações, nas mais variadas áreas da atividade humana. Muitas dessas inovações se apoiam intensivamente nas tecnologias da informação em comunicação (TIC) para que sejam materializadas e difundidas de forma global.

Nessa profusão que se assiste contemporaneamente, a Internet opera como espinha dorsal ao redor da qual o mundo digital tem surgido. Mais recentemente, essa espinha dorsal passou a possibilitar que quaisquer objetos pudessem a ela se conectar, levou conexão a novos tipos de sensores e abriu caminho em direção à Internet da Coisas ou *Internet of Things* (IoT).

Essas "coisas" passam a ser interconectadas a qualquer momento, em qualquer lugar, com qualquer outra "coisa", e usam qualquer caminho ou rede para prestar qualquer serviço (Borgia, 2014). A IoT abrange uma rede complexa, adaptativa e autoconfigurável, que interconecta "coisas" à Internet por meio de protocolos de comunicação normatizados (Da Silva *et al*., 2015).

As "coisas" interconectadas têm representação física ou virtual no mundo digital; contêm informações da identidade, *status*, localização e informações privadas ou sociais relevantes; capacidade de atuação e sensoriamento; funcionalidades de programação; identificação única e proporcionam serviços, com ou sem intervenção humana, coleta de dados, comunicação e capacidade de atuação (Minerva, Biru & Rotondi, 2015).

Estima-se que até 2020 seja atingido o número de 24 bilhões de dispositivos interconectados, gerando US$ 1,3 trilhão em oportunidades de receita apenas para operadoras de redes móveis, abrangendo segmentos verticais como saúde, educação, engenharias, serviços públicos e bens de consumo (Gubbi *et al.,* 2013).

No contexto da IoT, uma variedade de coisas ou objetos - como *tags* de identificação por radiofrequência (RFID - *Radio Frequency Identification*), sensores, atuadores, telefones celulares, entre outros, conseguem interagir entre si, além de cooperar com seus pares para alcançarem objetivos comuns, usualmente utilizando esquemas de endereçamentos exclusivos, como, por exemplo, o *Internet Protocol* (IP), (Atzori, Iera & Morabito, 2010).

Ao longo dos anos, a tecnologia RFID foi sendo aperfeiçoada, de modo que atualmente é utilizada em diversas aplicações comerciais e logísticas, seja para o gerenciamento do ciclo de vida de produtos ou para sua precificação; para rastreamento de origem-destino de encomendas ou para a implementação de procedimentos de prevenção de perdas no varejo. Equipamentos utilizados na área de saúde, modais de transportes de cargas e passageiros, agricultura e pecuária e todas as outras áreas da atividade humana podem se beneficiar dessa tecnologia.

Desde a Segunda Guerra Mundial, os princípios da tecnologia RFID foram utilizados como modo de identificação de aviões captados por radar, diferenciando os aviões "amigos" dos "inimigos" (Faccioni Filho, 2016). Muitas forças de segurança ao redor do mundo utilizam

essa tecnologia para realizar a gestão do ciclo de vida de seus ativos, como o faz o Departamento de Polícia de Hamburgo, Alemanha (Vaccarezza, 2012).

No Brasil, existe um sistema de controle de armamentos baseado apenas em seu número de identificação. Segundo dados do Instituto de Pesquisa Econômica Aplicada (IPEA, 2018), em 2015 houve uma média de 41.817 casos de homicídio no Brasil provocados por armas de fogo. Provavelmente esse índice seria reduzido se fossem adotadas medidas em diversos setores governamentais para incrementar o controle na fabricação, venda e compra de armamentos por meio da utilização de tecnologia de RFID associada a um software.

Algumas tentativas de um controle melhor na rastreabilidade de armamentos já foram realizadas no país. O programa "DNA das armas", por exemplo, teve como objetivo promover o debate sobre a necessidade de implantação de tecnologia capaz de melhorar o rastreamento das armas de fogo no Brasil e impedir que a simples raspagem do número de série impossibilitasse burlar a identificação da arma. Entretanto tal programa não vigorou.

O controle atual de armas no Brasil é realizado com base num banco de dados da Polícia Federal, o Sistema Nacional de Armas – SINARM. Nesse sistema são realizados cadastros de diversas naturezas, como autorizações de porte de arma de fogo expedidas pela Polícia Federal; cadastramento da identificação do cano da arma; características das impressões de raiamento e de microestriamento de projétil disparado, entre outras. Trata-se de um sistema de cadastro, sem maiores funcionalidades.

Esse cenário evidencia a importância do desenvolvimento de estudos que proponham o incremento na utilização de tecnologia RFID no âmbito do setor de Defesa, considerando que essa tecnologia, de custos relativamente baixos, permite grande precisão na identificação de objetos, facilidades de miniaturização e instalação e possibilidades de conectividade à Internet para o registro de dados em repositórios específicos (Finkenzeller, 2003).

Nesse contexto, este trabalho tem por objetivo realizar a proposição de um sistema de rastreamento de armamentos com base em sensores RFID. Sua contribuição visa atender à sociedade na busca de níveis de segurança aceitáveis, colaborar com as discussões para a ampliação do conhecimento sobre o assunto e adotar inovações com a aplicação de IoT na rastreabilidade de armamentos.

O trabalho está estruturado em cinco seções. Além dessa primeira seção introdutória, a segunda seção apresenta a metodologia de pesquisa adotada. A terceira seção traz a fundamentação teórica acerca da conceituação e aplicabilidade da IoT com especial atenção à área de Defesa e Segurança, a questão do rastreamento de armamentos e alguns casos exemplificadores de outros países. A quarta seção é dedica à apresentação do sistema de rastreamento de armamentos proposto. O trabalho é encerrado com a quinta seção, onde são feitas as considerações finais e sugestões para futuros estudos.

2. Metodologia Adotada

Para o desenvolvimento desse trabalho, optou-se por realizar uma pesquisa de natureza qualitativa e de caráter exploratório, com o intuito de alcançar maior proximidade de conhecimento e aplicação de um dado fenômeno sobre o qual ainda não se tem informações suficientes para se responder ao problema (Collis & Hussey, 2006).

Como fontes de dados, utilizou-se dados secundários fundamentalmente obtidos a partir de pesquisa bibliográfica, fundamentando a construção do referencial teórico e a exploração de possibilidades de solução para o problema. Segundo Collis & Hussey (2006: 87), a pesquisa bibliográfica é o "processo de explorar a literatura existente para averiguar o que já foi escrito

ou publicado sobre o tópico de pesquisa escolhido, como pesquisas anteriores foram realizadas e qual o seu impacto em seu próprio problema de pesquisa".

Nesse sentido, a pesquisa bibliográfica consistiu na busca por artigos, livros e estudos produzidos por organizações governamentais e não governamentais relativamente ao problema: utilização de IoT e/ou RFID como ferramenta para o rastreamento de armamentos.

Usualmente, a pesquisa qualitativa é concluída com a comunicação das análises e dos resultados (Collis & Hussey, 2006) o que, no caso desse trabalho, é feito por intermédio da descrição das tecnologias passíveis de utilização e das práticas de controles de armamentos, culminando com a proposição de um sistema para a resolução do problema. No caso específico do Brasil, são considerados os procedimentos atuais adotados para o monitoramento de armas.

3. Fundamentação Teórica

3.1 Internet das Coisas – IoT (Internet of Things)

O conceito de Internet das Coisas está fora do âmbito das tecnologias, pois não decorre delas, mas utiliza-as para exercer uma série de funcionalidades (Faccioni Filho, 2016). São diversas as tecnologias conexas ao "conceito"; por exemplo, as que se referem à conexão física dos objetos, ou de infraestrutura básica, demonstradas pelas conexões cabeadas e as conexões sem fio. Essas afirmações corroboram a definição de Vermesan & Friess (2013) que a IoT é conceito e um paradigma que considera a presença difusa no ambiente de uma variedade de coisas ou objetos que, por meio de conexões sem fio e com fio e esquemas de endereçamento únicos, são capazes de interagir uns com os outros e cooperar com outras coisas ou objetos para criar novos aplicativos ou serviços e alcançar objetivos comuns.

A IoT também pode ser definida como uma infraestrutura de rede global, que liga objetos físicos e virtuais por meio da exploração de capacidades de captura e comunicação de dados. Essa infraestrutura compreende a evolução da Internet e da rede existente, capaz de oferecer competência específica de identificação de objetos, sensoriamento e conexão como base para o desenvolvimento de serviços e aplicações cooperativas independentes. Elas serão caracterizadas por um alto grau de captura de dados autônomos, transferência de eventos, conectividade de rede e interoperabilidade (CASAGRAS, 2008).

Além de aumentarem a competitividade de diversos mercados verticais, as tecnologias de IoT podem proporcionar novas oportunidades de negócios: (i) conectando mercados verticais, originando aplicações e serviços transversais baseados no uso de uma plataforma comum de tecnologias de informação e comunicação; (ii) possibilitando o surgimento e crescimento de novos segmentos de mercado e aplicações, possibilitado pela capacidade de interagir com objetos físicos por meios digitais e (iii) otimizar processos de negócios utilizando técnicas avançadas de análise aplicadas a fluxos de dados (Miorandi *et al*., 2012).

Para Minerva, Biru & Rotondi (2015), a IoT é um domínio que integra diferentes tecnologias e campos sociais e de negócios. Nesse contexto, a IoT abrange uma rede complexa, adaptativa e autoconfigurável, que interconecta "coisas" à Internet por meio de protocolos de comunicação normatizados. As "coisas" interconectadas têm representação física ou virtual no mundo digital; contêm informações da identidade, status, localização e informações privadas ou sociais relevantes; capacidade de atuação/sensoriamento, funcionalidade de programação e identificação única; proporciona serviços, com ou sem intervenção humana, por meio de identificação única, coleta de dados, comunicação e capacidade de atuação.

De acordo com Miorandi *et al*. (2012), pode-se identificar alguns recursos principais no âmbito do sistema que a IoT precisa considerar:

(i) Heterogeneidade de dispositivos: a IoT será caracterizada por ampla heterogeneidade em termos de dispositivos que participam do sistema, os quais deverão apresentar capacidades muito distintas do ponto de vista computacional e de comunicação. O gerenciamento de um nível tão alto de heterogeneidade deve ser amparado nos âmbitos arquitetônico e de protocolo.

(ii) Escalabilidade: a medida que os objetos do dia a dia se conectam a uma infraestrutura de informação global, surgem problemas de escalabilidade em diferentes níveis, incluindo: (a) nomeação e endereçamento - devido ao tamanho do sistema resultante, (b) comunicação de dados e rede - devido ao alto nível de interconexão entre um grande número de entidades, (c) gestão da informação e do conhecimento - devido à possibilidade de construção de uma contraparte digital para qualquer entidade e / ou fenômenos no campo físico e (d) prestação e gestão de serviços - devido ao grande número de opções de execução de serviços / serviços que podem estar disponíveis e a necessidade de lidar com recursos heterogêneos.

(iii) Troca de dados ubíqua por meio de tecnologias sem fio de proximidade: em IoT, um papel proeminente será desempenhado pelas tecnologias de comunicação sem fio, permitindo que objetos inteligentes permaneçam em rede.

(iv) Soluções otimizadas para energia: para uma variedade de entidades de IoT, minimizar a energia a ser usada para fins de comunicação / computação será uma restrição primária. Embora as técnicas relativas à extração de energia (por exemplo, de materiais piezelétricos ou micropainéis solares) mitiguem os dispositivos das restrições impostas pelas operações da bateria, a energia será sempre um recurso escasso a ser manuseado com cuidado. Portanto a necessidade de criar soluções que otimizem o uso de energia (mesmo às custas do desempenho) se tornará cada vez mais atraente.

(v) Recursos de localização e rastreamento: devido ao fato de entidades em IoT poderem ser identificadas e fornecidas com recursos de comunicação sem fio de curto alcance, torna-se possível rastrear a localização (e o movimento) de objetos inteligentes no mundo físico. Aplicações em logística e gerenciamento de ciclo de vida de produtos, que já utilizam amplamente tecnologias de RFID.

(vi) Capacidades de auto-organização: a complexidade e dinâmica que muitos cenários de IoT provavelmente apresentarão chamadas para a distribuição de inteligência no sistema, fazendo com que objetos inteligentes (ou um subconjunto deles) possam reagir autonomamente a uma ampla gama de situações diferentes, a fim de minimizar a intervenção humana.

(vii) Interoperabilidade semântica e gerenciamento de dados: IoT será muito exigida para troca e análise de grandes quantidades de dados. Para transformá-los em informações úteis e para garantir a interoperabilidade entre diferentes aplicações, é necessário fornecer dados com formatos e modelos adequados e padronizados, e descrição semântica de seu conteúdo (meta-dados), usando linguagens e formatos bem definidos. Isso permitirá que os aplicativos de IoT sustentem o raciocínio automatizado, um recurso importante para permitir a adoção bem-sucedida de tal tecnologia em larga escala.

(viii) Mecanismos incorporados de segurança e preservação da privacidade: devido ao intenso complexo com o domínio físico, a tecnologia de IoT deve ser segura e preservar a privacidade por design. Isso significa que a segurança deve ser considerada uma propriedade-chave no sistema e ser levada em consideração no projeto de arquiteturas e métodos para soluções de IoT. Espera-se que isso represente os principais requisitos para garantir a aceitação pelos usuários e a ampla adoção da tecnologia.

3.2 Rastreabilidade

Segundo Moura *et al*. (2004), a rastreabilidade de materiais é um atributo que permite a identificação da origem de um item expedido, além do registro e rastreamento de peças, processos e materiais usados na produção, por meio de um número serial ou lote. O rastreamento, assim, define onde o produto se encontra durante o processo de produção. Quanto melhor o processo de rastreamento dos materiais, maior a garantia de gestão mais precisa dos inventários, permitindo o monitoramento da rastreabilidade de itens e tornando mais eficientes os processos.

De acordo com Lirani (2005), um sistema de rastreabilidade é uma ferramenta que possibilita identificar dados e fatos relativos a um produto durante o ciclo de sua cadeia produtiva, baseando-se no registro histórico dos acontecimentos que o envolvem. Nesse contexto, pode-se exemplificar a rastreabilidade a partir da montagem da árvore genealógica de uma família, em que são seguidos os "rastros" deixados pelos antepassados em registros de igrejas, cartórios, prefeituras, cemitérios e outros documentos. Ainda segundo o mesmo autor, existem alguns tópicos que devem ser considerados num sistema de rastreabilidade: a) codificação única que garanta a exclusividade da identificação do produto; b) esquema de armazenagem de informações; normalmente, um banco de dados; c) procedimentos que permitam o fácil registro das ocorrências na vida do produto; d) esquema de recuperação das informações registradas no banco de dados; e) registros mantidos em cada local de passagem do produto.

É importante ressaltar que um sistema de rastreabilidade não assegura a qualidade, tampouco evita ou resolve problemas ocorridos com o produto. Ele apenas recupera, de forma precisa, eficiente e rápida, seu histórico de localização e utilização, facilitando o serviço dos investigadores que pesquisam as causas da ocorrência em pauta (Lirani, 2005).

Segundo Metzner, Silva & Cugnasca (2014), a rastreabilidade pode ser definida como um sistema de identificação que permite resgatar a origem e a história do produto em todas as etapas da cadeia de suprimentos, referindo-se desde a produção da matéria-prima até o uso pelo consumidor final. Nesse contexto, amplas gamas de tecnologias podem ser empregadas para garantir a rastreabilidade do produto, agregadas aos processos de qualidade, como: códigos de barras, QR codes (do inglês, *Quick Response*) e RFID.

3.3 Radio Frequency Identification (RFID)

A tecnologia RFID usa ondas de rádio para identificar automaticamente pessoas ou objetos. Existem diversos métodos de identificação, porém o mais comum consiste em armazenar um número serial de identificação em um microchip ligado a uma antena (o chip e a antena juntos são chamados de *transponder* RFID ou *tag* RFID). A antena permite que o chip transmita a informação de identificação a um leitor. O leitor converte as ondas de rádio

refletidas da *tag* RFID em informações digitais, que por sua vez podem ser transmitidas a computadores que podem fazer uso delas.

Em resumo, um leitor modula uma determinada frequência de rádio, transmite informações para uma *tag* que, por meio de um elemento de acoplamento, repassa-as para o seu *microchip*. Quando a *tag* não possui uma bateria própria, a energia é fornecida pelo leitor por meio das ondas de rádio, o que permite que ela só permaneça ativa quando estiver na área de cobertura do leitor. Assim, a comunicação ocorre por meio da radiofrequência, em ambos os sentidos (Zimpel *et al*., 2015).

O sistema RFID possui dois componentes principais: a *tag* e o leitor. A *tag* é aplicada diretamente a um objeto que a identifica. Já o leitor é o elemento que colhe dados da *tags* e os transmite à Internet. Os padrões RFID estão relacionados tanto aos protocolos de frequência (para comunicação de dados) quanto ao formato de dados (para armazenamento de dados na *tag*).

3.4 Controle de Armamentos

Nos EUA, o controle da venda e posse de armas em âmbito federal é efetuado pelo BATF e, em certos aspectos, pelo FBI. Já na esfera estadual e local, o controle é exercido por forças policiais e procuradorias em suas funções de aplicação da lei. Existem três associações de polícia nos EUA: *National Association of Chiefs of Police, American Federation of Police e a National Police Ofticers Association of America*, todas sutilmente favoráveis a um maior controle de armas. Quanto à sociedade, o controle acaba sendo muito influenciado por inúmeras Organizações Não Governamentais (ONG) que se dedicam a pressionar o Congresso para mudanças nas leis tanto a favor quanto contra um controle maior (Bueno, 2001).

Apesar de frequentemente ser comentada a facilidade na aquisição de armas nos EUA, existem mais de 20.000 leis de controle nos códigos americanos, em sua maioria leis estaduais e locais, tratando de regulamentações menores. Mesmo havendo essa infinidade de leis, o sistema de rastreamento das armas de fogo ainda não é tão eficaz.

Estima-se que existam mais de 393 milhões de armas de fogo de propriedade civil nos Estados Unidos. Isso contribui para que cada homem, mulher e criança possua uma e ainda sobre 67 milhões de armas (KARP, 2018). Nesse contexto, é impossível o cálculo preciso, tendo em vista que a maior parte não é registrada, além do fato de cada estado possuir seus próprios métodos de registro (Bueno, 2001).

Em 2005 foi criado um sistema digital de rastreamento pelo governo americano, utilizado por oficiais do Escritório de Armas, Tabaco, Armas de Fogo e Explosivos (ATF, na sigla em inglês) do Departamento de Justiça dos EUA. O sistema é chamado *e-trace (Sistema Eletrônico de Rastreamento)*, baseado na internet, e permite que as agências de segurança da lei submetam dados de rastreamentos de armas de fogo ao Centro de Rastreamento Nacional (NTC) do ATF.

Apenas os usuários autorizados podem receber resultados de rastreamento de armas de fogo por meio do e-trace, pesquisar em seus bancos de dados os rastreamentos de armas enviados por sua agência individual e realizar funções analíticas (ATF ONLINE, 2018). Esse sistema atua na identificação da origem de armas de fogo apreendidas em operações policiais, revelando o mapeamento do trajeto realizado pelas armas desde a compra original, passando por todos os seus registros até a apreensão. Essa ferramenta foi gerada para auxiliar

investigações criminais nos Estados Unidos e no exterior, tanto pela identificação de donos das armas, de possíveis traficantes e de rotas ilegais.

O *e-trace* permite que oficiais possuam "uma plataforma de informação para desenvolver as melhores estratégias de investigação para reduzir a criminalidade e a violência relativas a armas de fogo". Entretanto, ao disponibilizar o sistema para outro país, é necessário estar ciente de que as informações resultantes das operações realizadas alimentarão o banco de dados do governo americano, que já o exportou para mais de 40 países, especialmente para Caribe, América Latina e Europa (Senra, 2017).

Nas Forças Armadas dos Estados Unidos da América (EUA), pode ser identificada a necessidade que a defesa possui quanto à IoT. Nesse caso tem-se procurado adotar medidas diferentes. A criação de um construto organizacional que permita uma parceria homem-máquina efetiva, estabelecendo uma ação de acordo com o comando e a cultura das Forças Armadas desse país é cada vez mais notória.

A criação e implementação de tal construção de comando e controle, em vez de simplesmente executar comandos diretos, passarão a receber objetivos de futuros conjuntos de dispositivos e máquinas conectados, e interpretarão, no âmbito do sistema, como os dispositivos, sensores e capacidades funcionam como uma equipe para realizar o objetivo comandado (Palmer, Fazzari & Wartenberg, 2016).

No Texas, a *Richardson Police Department* (RPD), Departamento de Polícia da cidade de Richardson, começou a empregar em 2013 uma solução para rastreamento de ativos por meio da tecnologia RFID. Tal atitude teve como objetivo melhorar a eficiência, reduzir custos e proteger melhor uniformes, armas e outros equipamentos utilizados pela polícia. Com a implantação do sistema, o departamento passou a deduzir meia hora do tempo que levava para verificar todos os equipamentos dentro de uma viatura, etapa realizada no início e no final de um turno. Acredita-se que o sistema não apenas melhorou o trabalho da polícia, como o departamento estima que economizou cerca de US$ 9,000 por viatura no ano, fruto da redução dos custos e ganhos de eficiência (Bacheldor, 2013).

Para as armas de fogo e outros itens que necessitam de *tags* de baixo perfil, o departamento está empregando a *Xerafy Titanium Metal Skin*, uma pequena e fina etiqueta RFID, com dimensões de 45 mm x 5,6 mm x 0,8 mm. De acordo com Pearson, todas as *tags* são pré-codificadas com um único número de série. As espingardas levadas dentro de cada viatura são um exemplo de arma que recebem etiquetas *Titanium Metal Skin*, permanentemente seladas no interior dos itens, enquanto os rifles têm *Xerafy Versa Trak tags* (Bacheldor, 2013).

3.4.1 Controle de Armas na Grã-Bretanha

Em 1920, após o trabalho em conjunto de um comitê reservado, liderado por Sir Ernley Blackwell, com a polícia para discutir uma forma de controle de armamentos, foi introduzido o *Firearm Act* que por sua vez introduziu o *Firearm Certificate*. Este certificado serviria como licença e ao mesmo tempo como documento de registro de todas as armas, com algumas exceções (Bueno, 2001).

Em 1967 foi aprovado o *Criminal Justice Act*, em função do aumento generalizado da violência e dos crimes com armas nos anos de 1960. Passou-se a exigir o *Shotgun Certificate* para a aquisição de cartucheiras de cano longo; a polícia poderia recusar também o certificado caso julgasse que a posse de arma por determinada pessoa ameaçasse a segurança pública, ou seja, a licença para a compra passou a ser individualizada e condicionada à avaliação dos antecedentes e da sanidade mental do requerente (Bueno, 2001).

Na Grã-Bretanha, existem quatro níveis de segurança: (i) armas que não são "de fogo" e que possuem baixo poder de destruição (exemplo: armas de ar comprimido). Para essas não se exige nenhum certificado; (ii) armas denominadas cartucheiras que exigem o *Shotgun Certificate*; (iii) revólveres, pistolas, carabinas, rifles, cartucheiras de repetição, armas de ar comprimido de alto poder e outras consideradas extremamente perigosas, que exigem o *Firearm Certificate* e (iv) armas que não possuem certificado e necessitam de autorização especial do Secretário de Estado para o seu uso ou porte. Nesse contexto, estão as armas reservadas ao uso da polícia, agentes de segurança e forças armadas como também as armas já banidas (Bueno, 2001).

Os certificados, em ambos os casos, têm um prazo de validade de 5 anos. A forma de controle e consequente forma de rastreamento dá-se por meio de dados contidos no *Firearm Certificate*. Este é responsável pela especificação do número das armas e tipo de munições que podem ser adquiridas, além das condições e locais de uso e condições e forma de armazenar em residências. Quanto ao *Shotgun Certificate*, esse não limita o número de armas nem os locais de tiro (Bueno, 2001).

3.4.2 Controle de Armas na Alemanha

Segundo dados disponíveis no site Terra, obter licença para possuir arma de fogo, a chamada *Waffenschein*, na Alemanha não é muito fácil. O indivíduo deve comprovar, de forma concreta, que corre risco ou que tem de garantir a segurança de um objeto, o que se aplica a políticos ou serviços de segurança. Porém, mesmo que tenha sido dada a permissão, o porte é restringido, por exemplo, em festas e eventos. Além disso, a cada três anos, a fiabilidade do cidadão é verificada, e pode ser retirada por diversos motivos, como multa recebida equivalente a 60 dias ou mais do salário líquido, ou pena de prisão de ao menos um ano (DW, 2017).

O Departamento de Polícia de Hamburgo, Alemanha, trabalha num projeto para se usar um sistema de identificação de radiofrequência (RFID), por meio de pequenas etiquetas e *chip* RFID incorporados a coletes à prova de balas e a armas de fogo usados por policiais. Nesse contexto, um *software* é utilizado para controlar e gerenciar os itens. O sistema identifica automaticamente e registra cada equipamento durante a entrada e saída dos policiais do departamento, além de rastrear as armas e coletes à prova de balas, enquanto os policiais estiverem em plantão (Vaccarezza, 2012).

3.5 Contexto do Controle de Armas no Brasil

Para que as armas de fogo possam ser utilizadas, existe uma série de requisitos que regulamentam seu controle. No Brasil, as armas de fogo sempre foram controladas direta ou indiretamente pelo Exército. O primeiro documento a especificar as regras sobre fabricação e circulação de armas e munições na República foi o Decreto Presidencial n.º 24.602 de 06 de julho de 1934, posteriormente regulamentado pelos Decretos nº. 1.246 de 11 de dezembro de 1936, n.º 47.587 de 04 de janeiro de 1960 e n.º 94 de 30 de outubro de 1961 (Dias, 2003).

Durante o governo de Getúlio Vargas, existiam as empresas particulares que, em sua maioria, fabricavam armas, cartuchos e munição de caça ou de explosivos. Para conseguirem licença de funcionamento, era necessário submeter-se quase às mesmas restrições que o governo federal fazia às empresas exclusivamente autorizadas a fabricar armas e munição de guerra, ou seja, deveriam submeter-se a quaisquer condições que o governo federal julgasse

conveniente para a comercialização de seus produtos, tanto para o público brasileiro quanto para o estrangeiro, assim como para as importações de matérias-primas (Dias, 2003).

Em 28 de janeiro de 1965, o Decreto n.º 24.602 foi revogado pelo Decreto n.º 55.649, cujo nome era Regulamento para o Serviço de Fiscalização e Legislação para controle de armas leves no Brasil: Importação, Depósito e Tráfego de Produtos Controlados pelo Ministério da Guerra (SFIDT) – R105. Como envolvia regras também sobre fabricação e comércio, mais tarde, em 1983, esse decreto teve seu nome alterado para Regulamento para a Fiscalização de Produtos Controlados (alteração feita pelo Decreto n.º 88.113 de 21 de fevereiro de 1983). A fiscalização dos chamados produtos controlados – armas, munições, explosivos e agentes químicos – sempre foi exercida pelo Exército, ou seja, sem qualquer controle paralelo por parte de instituições civis (Dias, 2003).

Em 20 de fevereiro de 1997, passa a vigorar a Lei n.º 9.437, primeira lei a tratar sobre o uso de armas por civis e estabelecer tanto esse controle quanto o cadastro do que era produzido, vendido e importado. Tal controle passou a ser exercido pelo Ministério da Justiça, e não de maneira pulverizada pelas polícias do país. A propriedade e o porte de armas por civis anteriormente eram direitos reservados apenas aos que fossem considerados idôneos pelas autoridades policiais; assim, os registros e portes de armas para civis eram concedidos pelas polícias de seus estados (Dias, 2003).

A Lei n.º 9.437 foi responsável, também, pela criação do SINARM, setor da Polícia Federal criado para agrupar todas as informações sobre armas de civis. Nesse sentido, quem desejasse obter autorização para comprar uma arma, deveria solicitá-la à autoridade policial de seu estado, que consultaria o SINARM para, então, deferir ou indeferir o pedido. No registro de sua arma constariam as seguintes informações: a) nome completo e filiação; b) endereços residencial e de trabalho; c) profissão; d) número de documentos de identidade e data de expedição; e) nomes do fabricante e do vendedor da arma; f) número e data da nota fiscal; g) tipo, marca, modelo e número de série da arma; h) calibre e capacidade dos cartuchos; i) modo de funcionamento; j) quantidade de canhões e largura; k) tipo de alma (se lisa ou raiada); l) quantidade de raias e sentido (Dias, 2003).

Após a incorporação do Estatuto do Desarmamento (Lei n.º 10.826), aprovado em 09 de dezembro de 2003, o SINARM passou a ter, além das existentes, as seguintes funções:

> a) cadastrar as autorizações de porte de arma de fogo e as renovações expedidas pela Polícia Federal;
> b) cadastrar as ocorrências oriundas de fechamento de empresas de segurança privada e de transporte de valores que possam vir a alterar os dados cadastrais;
> c) cadastrar os armeiros em atividade no País e conceder-lhes licença para exercer a atividade;
> d) cadastrar, mediante registro, os produtores, atacadistas, varejistas, exportadores e importadores autorizados de armas de fogo, acessórios e munições;
> e) cadastrar a identificação do cano da arma, as características das impressões de raiamento e de microestriamento de projétil disparado, conforme marcação e testes obrigatoriamente realizados pelo fabricante; f) informar às secretarias de Segurança Pública dos estados e do Distrito Federal os registros e autorizações de porte de armas de fogo nos respectivos territórios, bem como manter o cadastro atualizado para consulta (Dias, 2003).

Outras questões importantes provenientes do Estatuto referem-se a: a) a obrigatoriedade de todas as munições produzidas no país saírem das fábricas em caixas com código de barras, para que seja possível identificar o fabricante e o adquirente; b) a obrigatoriedade de órgãos de segurança pública comprarem munição com identificação do lote e do adquirente no culote dos projéteis; c) a obrigatoriedade de os fabricantes de armas gravarem-nas com dispositivo intrínseco de segurança e de identificação a partir de 23 de dezembro de 2004; d) a obrigatoriedade da destruição de armas apreendidas quarenta e oito horas após terem sido liberadas pelo juiz responsável pelo processo a elas pertinente; e) a proibição de compra de armas por menores de vinte e cinco anos; f) as campanhas de anistia e recompra de armas (DIAS, 2003).

Em 2011, a empresa brasileira Condor criou um *chip* que permitia rastrear armas. O *chip* deve ser instalado no momento da composição do produto e, no caso da granada não letal da empresa, foi aplicado na peça que carrega o grampo de segurança (argola que aciona o explosivo), conhecida como Espoleta de Ogiva de Tempo (EOT). A tecnologia permite o controle logístico de distribuição, estoque e validade dos produtos. A fabricante garantiu que esse sistema é exclusivo e a tecnologia inviolável, ou seja, qualquer tentativa de adulteração torna o artefato inoperante. Com tal tecnologia, seria possível saber de onde o explosivo saiu, além de trazer informações como os dados da compra e de estoque. Dessa forma, seria possível também identificar roubos, furtos e qualquer desvio do destino do armamento (Salme, 2011).

Em 2015, houve uma tentativa de introduzir um programa capaz de rastrear armas. Tal programa foi intitulado "O DNA das Armas". Inspirado numa parceria entre o Instituto Sou da Paz e o Ministério Público de São Paulo, o programa acabou não evoluindo no Plano Nacional de Segurança Pública. A ideia tinha como objetivo promover o debate sobre a necessidade de implantação de tecnologia capaz de melhorar o rastreamento das armas de fogo no Brasil e impedir que a simples raspagem do número de série impossibilitasse a identificação da arma. O "DNA" poderia ser aplicado na forma de um registro em várias partes da arma, impossível de se ver a olho nu, de modo que a supressão da identificação da arma só seria possível caso ela fosse destruída (Julião, 2017).

Após a criação do SINARM, foi possível realizar uma padronização no gerenciamento de informações em três dimensões: 1) armas - contemplando os seguintes quesitos: número de série, modelo, tipo, ano de fabricação, calibre, tipo de raias; 2) proprietário - nome, endereço, ocupação, qualificações, e; 3) eventos- classificados em roubo, furto, perda, desvio, venda, transferência, doação. Nesse contexto, as duas primeiras possuem função de cadastro e a última tem por função estabelecer os eventos possíveis entre as duas primeiras dimensões (Bueno, 2001). Vale dizer que o único sistema de cadastro que não repassa suas informações ao SINARM é o cadastro do Ministério do Exército que, além do seu arsenal, realiza o registro e o controle das armas de uso de esportistas, caçadores e colecionadores cujos calibres não são permitidos aos civis (Bueno, 2001).

4. Proposição de um Sistema de Rastreamento de Armamentos

4.1 Antecedentes

Em 2011, o então Secretário-Geral das Organização das Nações Unidas (ONU) chamou atenção para a estatística de violência, afirmando que ela poderia assumir proporções assustadoras em comunidades em que a circulação de armas fosse grande. Tal conclusão já

Avaliado pelo sistema double blind review
Editor: Marcelo G. Amaral

havia sido assinalada pela ONU, ainda em 2006, no Relatório Mundial sobre Violência contra Crianças, elaborado pelo brasileiro Paulo Sérgio Pinheiro (UNODC, 2011).

Além da violência, também foi levantada a questão do controle inadequado dos estoques de munições como responsável por uma parte substancial do abastecimento dos mercados ilegais.

Nesse sentido, o secretário Ban Ki-moon declarou em seu relatório que "o Conselho de Segurança poderia incentivar os Estados a fortalecer sua capacidade de rastreamento [de armas leves e munições] e reforçar a cooperação internacional no que diz respeito ao rastreamento nesse contexto, inclusive com as Nações Unidas" (UNODC, 2011). A falta de controle de armas fomenta conflitos armados.

Ban Ki-moon diz ainda**:** "Em tais contextos, é fundamental que as medidas tradicionais de controle de armas sejam integradas às intervenções que visam à busca de armas e à melhoria da capacidade das autoridades de governo para reforçar a segurança das comunidades, administrar conflitos e reduzir a violência" (UNODC, 2011).

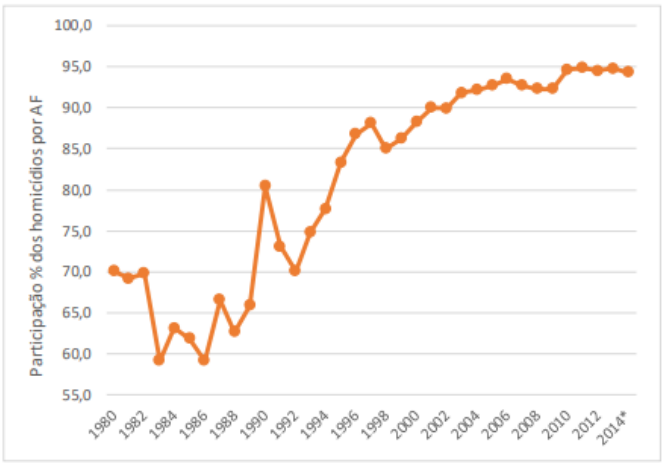
Após a aprovação do Estatuto do Desarmamento no Brasil, a Figura 1 demonstra que o número de homicídios tende à estagnação, diferente dos números ascendentes encontrados de 1980 até 2004. Em contrapartida, cresce o uso das armas de fogo como instrumento para perpetrar homicídios (Waiselfsz, 2016), como demonstrado na

Figura 1 - Participação dos homicídios por arma de fogo no total de óbitos.
Fonte: WAISELFSZ, 2016.

Ano	%
1980	70,1
1981	69,2
1982	69,8
1983	59,2
1984	63,2
1985	61,9
1986	59,2
1987	66,6
1988	62,7
1989	65,9
1990	80,5
1991	73,1
1992	70,1
1993	74,8
1994	77,7
1995	83,3
1996	86,8
1997	88,1

Ano	%
1998	85,0
1999	86,2
2000	88,2
2001	90,0
2002	89,9
2003	91,8
2004	92,1
2005	92,7
2006	93,5
2007	92,7
2008	92,3
2009	92,3
2010	94,6
2011	94,8
2012	94,5
2013	94,8
2014*	94,3

* Dados preliminares.



As tecnologias que fazem parte do conceito de Internet das Coisas pode ser aplicada à uma grande variedade de equipamentos militares, como veículos, suprimentos e até mesmo sistemas de armas (Wrona,2015). A tecnologia RFID permite identificar os objetos móveis de alta velocidade e muitas informações ao mesmo tempo, possui vida útil longa e grande capacidade de memória. É a tecnologia-chave dos artigos que abordam a tecnologia subjacente da IoT (Zhang *et al.*, 2012).

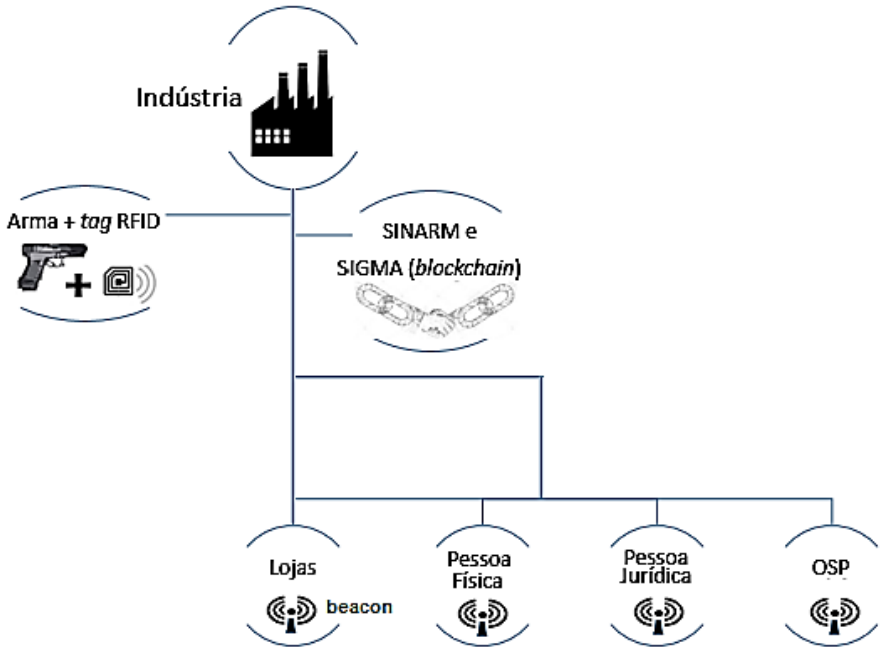
Avaliado pelo sistema double blind review
Editor: Marcelo G. Amaral

4.2 Caracterização do Sistema Proposto

Como notado ao longo deste trabalho, diversos países estão investindo em tecnologia RFID como controle em Defesa. A aplicabilidade do RFID em rastreabilidade de armamentos torna-se possível devido ao tamanho reduzido das *tag*s, para agilizar os processos desde sua fabricação até sua distribuição. A digitalização de um item equipado com RFID pode retornar uma variedade de dados, incluindo o fabricante, informações sobre o item, qual fornecedor proveu, o custo específico associado ao item, o caminho necessário para chegar à loja, bem como uma ampla variedade de outros dados relevantes (Ayoade, 2007).

Outro ponto importante onde o RFID pode ajudar é na detecção de armas em áreas públicas com o objetivo de proporcionar maior segurança (Hussein & Hu, 2016). A Figura 2 apresenta de forma diagramática o sistema proposto.

Figura 2 - Fluxo do sistema proposto.
Fonte: Autores.



O ponto de partida está na indústria que confecciona o armamento e instala a *tag* RFID no momento da composição da arma, numa parte que não seria divulgada por segurança. Caso houvesse tentativa de remoção ou destruição do *chip*, por exemplo, com excesso de frio, calor ou choques fortes no conjunto, esses estímulos também danificariam a usabilidade da arma. Após a confecção de uma arma, a indústria passaria todos os respectivos dados aos sistemas SIGMA e SINARM.

As pessoas, físicas e/ ou jurídicas, bem como Órgãos de Segurança Pública (OSP), poderiam adquirir a arma tanto a partir da indústria quanto das lojas. Leitores de RFID poderiam ser posicionados em pórticos instalados na entrada de quartéis, em viaturas das Polícias Federal,

Civil e Militar, em ruas, avenidas e rodovias, para que fosse possível detectar a presença da arma em qualquer um desses locais.

5. Considerações Finais

O presente estudo foi desenvolvido baseado no contexto da rastreabilidade de armas de fogo. Para que fosse possível atingir o objetivo proposto e responder ao problema de pesquisa, realizou-se a revisão da literatura e de documentos sobre o assunto. Constatou-se que o controle das armas de fogo baseado apenas em identificação numérica que pode ser facilmente raspada e consequentemente eliminada torna o controle deficiente, colocando em riscos questões de segurança e bem-estar da população. A ausência de controle nesse campo torna a segurança cada vez mais sensível. O índice de mortes por armas de fogo é crescente a cada ano, bem como o contrabando e roubo de armamentos. Nesse sentido, o controle desde a produção de armamentos até sua distribuição torna-se uma forma eficaz de evitar tais problemas.

Ademais, a revisão de literatura permitiu compreender não só as tecnologias aplicadas em IoT e RFID como também a rastreabilidade por meio dessas tecnologias. A adoção de sensores RFID associados a armamentos poderá facilitar o controle e cadastramento de armas, permitindo que sejam facilmente rastreadas, desde o momento de sua fabricação até a aquisição por proprietário final, seja pessoa física ou jurídica. Essa tecnologia poderá promover uma redução de ocorrências em diversos setores, como a diminuição do tráfico de armas. Já que se pode mapear e rastrear a localização do armamento, será possível intervir em tal ato. Outro exemplo acontece no roubo de armamentos, que seria significativamente reduzido, uma vez ser possível seu rastreamento pelas forças policiais. Acredita-se que, ao ser empregada tal tecnologia, a violência também diminuirá significativamente, pois haverá menos cidadãos com posse de armas.

O sistema proposto nesse trabalho não tem a pretensão de ser exaustivo, muito menos ser a solução total para cercear a violência no país. Porém, a partir de um controle maior da circulação das armas legais no país, seria possível desenhar um mapa de calor de zonas mais perigosas e cruzá-lo, por exemplo, com as zonas de maior incidência de armas. E, ao se cruzarem esses dados com dados de violência urbana e dados de redes móveis de celulares, seria possível serem solucionados mais crimes, além de tornar mais efetivas as políticas públicas de segurança. Nesse sentido, os modelos preditivos seriam melhores e melhor alimentados com esse grande volume de dados.

A partir dos resultados obtidos, futuros estudos podem focar na aplicação de tecnologias baseadas em aprendizado de máquina e ciência de dados para auxiliar no desenho de modelos preditivos; utilização de equipamentos ativos de baixo consumo para rastreamento em tempo real.

Referências

ATF ONLINE. (2018). *E-trace 4.0*. Recuperado em 20 de junho de 2018 de < https://etrace.atf.gov/etrace/ >.

Atzori, L., Iera A. & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54, p. 2787–2805.

Avanco, L., Guelfi, A. E., Pontes, E., Silva, A. A. A., Kofuji, S. T. & Zhou F. (2015) An effective intrusion detection approach for jamming attacks on RFID systems. *International EURASIP Workshop on RFID Technology (EURFID),* p. 73-80.

Ayoade, J. (2007). Privacy and RFID Systems Roadmap to solving security and privacy concerns in RFID systems. *Computer Law & Security Report*, 23, p. 555–561.

Bacheldor, B. (2018). *RFID otimiza tempo de policiais no Texas. O Departamento de Polícia da cidade de Richardson rastreia armas e equipamentos eletrônicos etiquetados com tags da Xerafy.* Recuperado em 20 de junho de 2018 de < http://brasil.rfidjournal.com/noticias/vision?106272013 >.

Bastos, D. A. & Silva, F.M. (2017). *Estudo e implementação de controladores para sistema RFID*. Recuperado em 10 de junho de 2018 de http://bdm.unb.br/bitstream/10483/859/1/2007_D%C3%A9boraBastos_Fl%C3%A1viaSilva.pdf >.

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications,* 54, p. 1-31.

Bueno, L. (2001). Controle de armas: um estudo comparativo de políticas públicas entre Grã-Bretanha, EUA, Canadá, Austrália e Brasil. *Dissertação (Mestrado em Administração Pública e Governo)* - FGV - Fundação Getúlio Vargas, São Paulo.

CASAGRAS - Coordination and Support Action for Global RFID-related Activities and Standardization. (2008). *CASAGRAS Says the Internet of Things should be more than RFID.* Recuperado em 20 de junho de 2018 de < http://www.rfidjournal.com/articles/pdf?4461 >.

Collis, J & Hussey, R. (2006). *Pesquisa em administração: um guia prático para alunos de graduação e pós-graduação*. 2. ed. Porto Alegre: Bookman.

Da Silva, A., Júnior, C., Santos, R., Martins, R. & De Oliveira, W. (2018). Criatividade e inovação: Internet das Coisas (IoT – Internet of Things). *Revista Expressão*. Recuperado em 7 de junho de 2018 de < http://www4.faculdadepromove.br/expressao/index.php/files/article/view/59 >.

Dias, C.I. (2018). *Legislação para controle de armas leves no Brasil: de Vargas a Lula***.** Recuperado em 18 de junho de 2018 de < http://comunidadesegura.org.br/files/active/0/armas_vitimas_legislacao.pdf >.

DW. (2018). *Como outros países regulamentam o porte de armas de fogo.* Recuperado em 18 de junho de 2018 de < https://www.dw.com/pt-br/como-outros-pa%C3%ADses-regulamentam-o-porte-de-armas-de-fogo/a-41555596 >.

Faccioni Filho, M. (2016). *Internet das Coisas*. Palhoça: Unisul Virtual.

Finkenzeller, K. (2003). RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. *John Wiley & Sons*.

Georg, N.J., Kelner, L. & Silvino Júnior, J.B. (2011). Armas de Fogo: Aspectos Técnicos Periciais. *Revista Jurídica*, 15(30), p. 137 – 156.

Gonçalves, R. (2018). *Idade dos Metais*. Recuperado em 10 de abril de 2018 de < https://historiadomundo.uol.com.br/pre-historia/idade-metais.htm> .

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems,* 29(7), p. 1645-1660.

Hussein, N. J. & Hu, F. (2016). An alternative method to discover concealed weapon detection using critical fusion image of color image and infrared image". *First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, p. 378-383.

IPEA. (2018) *Homicídios por Armas de Fogo Brasil.* Recuperado em 10 de abril de 2018 de < http://www.ipea.gov.br/atlasviolencia/dados-series >.

Julião, L.G. (2018). *Implantação do 'DNA das Armas' para identificação de armas de fogo e munição.* Recuperado em 10 de abril de 2018 de < https://blogs.oglobo.globo.com/eissomesmo/post/implantacao-do-dna-das-armas-para-identificacao-de-armas-de-fogo-e-municao.html>.

Karp, A. Estimating Global Civilian HELD Firearms Numbers. Disponível em: <http://www.smallarmssurvey.org/fileadmin/docs/T-Briefing-Papers/SAS-BP-Civilian-Firearms-Numbers.pdf>. Acesso em: 26 ago 2019.Lirani, A.C. (2005). Rastreabilidade, uma exigência comercial. *Visão Agrícola***,** 3, p. 97-99.

Metzner, V.C.V., Silva, R. F. & Cugnasca, C.E. (2018). *Modelo de rastreabilidade de medicamentos utilizando RFID, RSSF e o conceito de internet das coisas*. Recuperado em 10 de abril de 2018 de < http://roitier.pro.br/wp-content/uploads/2017/09/AC267.pdf >.

Minerva, R., Biru, A. & Rotondi, D. (2015). Towards a Definition of the Internet of Things (IoT). *IEEE Internet Initiative - Telecom Italia.* **27 maio 2015**. Recuperado em 20 de março de 2018 de < https://pt.scribd.com/doc/306069323/IEEE-IoT-Towards-Definition-Internet-of-Things-Revision1-27MAY15 >.

Miorandi D., Sicari S., Pellegrini F. & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10, p. 1497–1516.

Morris, D. S. & Glover, K. (2007). RFID Potential for Army Field Operations. *MILCOM 2007 - IEEE Military Communications Conference*, p. 1-4.

Moura, R. A. *et al.* (2004). *Dicionário de logística*. São Paulo: Imam.

Palmer, D., Fazzari, S. & Wartenberg, S. (2016). Defense Systems and IoT: Security Issues in an Era of Distributed Command and Control. *GLSVLSI '16, May 18 - 20,* p. 175-179.

Salme, F. (2011). *Segurança: Brasil cria chip rastreador de armas.* Recuperado em 18 de junho de 2018 de < http://www.advivo.com.br/blog/antonio-ateu/seguranca-brasil-cria-chip-rastreador-de-armas >.

Senra, R. (2017). *EUA treinarão policiais federais no Brasil para rastreamento de armas.* Recuperado em 20 de março de 2018 de < https://www.bbc.com/portuguese/brasil-40671348.

UNODC. (2011). *Rastreamento de armas leves é estratégico para redução da violência, afirma Secretário-Geral da ONU*. Recuperado em 18 de junho de 2018 de < http://www.unodc.org/lpo-brazil/pt/frontpage/2011/04/26-rastreamento-de-armas-leves-e-estrategico-para-reducao-da-violencia-afirma-secretario-geral-da-onu.html >.

Vaccarezza, C. (2012). *Inteligência Estratégica*. Recuperado em 20 de junho de 2018 de <http://csie-esg.blogspot.com/2012/04/rastreamento-de-armas-em-2006-o-comando.html >.

Vermesan, O. & Friess, P. (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. Aalborg: River Publishers Series in Communications.

Waiselfsz.J.J. (2016). *Mapa da Violência 2016 homicídios por armas de fogo no Brasil.* Recuperado em 20 de março de 2018 de < https://www.mapadaviolencia.org.br/pdf2016/Mapa2016_armas_web.pdf >.

Wrona, K. (2015).Securing the Internet of Things a military perspective. *IEEE 2nd World Forum on Internet of Things (WF-IoT)*, p. 502-507.

Zhang, K., Ao, Z., Tang, C., Wang, Y., Zhu, W. & Feng, B. (2012). Application of Internet of Things in Combined Operation Logistics Support. *Fourth International Conference on Computational and Information Sciences*, p. 388-391.

Zimpel, C., Rossetto, F.G., Hermes, M.M. & Nesi, V. (2015). RFID e rastreabilidade de estoque. *PR Coop. Tecn. Cient*, 11(130), p. 16-25.