Atualização da doutrina de gerenciamento de crises: incidentes policiais e centros de consciência situacional C5I na quarta revolução industrial

Paulo Augusto Aguilar
Mestre em Ciências Policiais de Segurança e Ordem Pública pelo Centro de Altos Estudos de Segurança "Cel PM Nelson Freire Terra" (PMESP). Capitão de Polícia Militar do Estado de São Paulo.
E-mail: aguilar.paulo@uol.com.br

RESUMO

O presente artigo tem como objetivo abordar a atualização de gerenciamento de crises. Trata-se de um tema bastante importante para a atividade policial, pois visa expandir a possibilidade das polícias brasileiras, seja militar, civil ou federal, de investigar delitos diversos, relacionados à segurança pública, ao fornecer conceitos de Big Data, Data Mining, Data Storytelling e Business Intelligence (BI) como forma de gerar melhor consciência situacional e imagem operacional comum de incidentes de todos os tipos e tamanhos, tudo isso com a flexibilidade de aplicativos disponíveis em smartphones, em tempo real, agilizando a capacidade de resposta e de adaptação do Estado por meio da aplicação do termo utilizado para descrever cenários caracterizados por volatilidade (volatility), incerteza (uncertainty), complexidade (complexity) e ambiguidade (ambiguity): (VUCA).

Palavras-chave: Gerenciamento de crises. Gerenciamento de incidentes. Centros de consciência situacional. VUCA.

ABSTRACT

This article aims to address the crisis management update. This is a very important theme for police activity, as it aims to expand the possibility of Brazilian police, whether military, civil or federal, to investigate various crimes related to public security by providing concepts of Big Data, Data Mining, Data Storytelling and Business Intelligence as a way to generate better situational awareness and common operational imagery of incidents of all types and sizes, all with the flexibility of real-time smartphone applications, streamlining state responsiveness and adaptability against VUCA, used to describes scenarios characterized by volatility, uncertainty, complexity and ambiguity.

Keywords: Crisis Management. Incidents Management. Centers of situational awareness. VUCA.

1 INTRODUÇÃO

No contexto policial, a doutrina de Gerenciamento de Crises e a sua definição foram introduzidas, em meados da década de 1990, por meio de duas publicações: Monteiro (1994) e Souza (1995). Souza (1995, p. 10), em sua obra, citou a definição de crise adotada pela *Federal Bureau of Investigation* (FBI), dos Estados Unidos da América (EUA), a saber: "Um evento ou situação crucial que exige uma resposta especial da Polícia, a fim de assegurar uma solução aceitável". Estudo que seguiu a dogmática utilizada pelo FBI, que encontra laços perenes até hoje no Brasil, e a sua utilização é unânime pelas polícias de todo o país.

Vale notar que, antes disso, a doutrina de Gerenciamento de Crises adotada pelo FBI sofreu um significativo aperfeiçoamento, em decorrência do incidente conhecido como "Cerco de Waco", ocorrido em 19 de abril de 1993, durante o cumprimento de um mandado de busca pelo *Bureau of Alcohol, Tobacco, Firearms and Explosives*, na cidade de Waco, no estado do Texas (EUA), que durou 51 dias e resultou na morte de 80 pessoas. Dois anos mais tarde, em 21 de maio de 1995, com a edição da *Presidential Decision Directive* 39 (PDD-39) – *Policy on Counter Terorism*, o FBI aumentou as suas atribuições a respeito do gerenciamento de incidentes terroristas (KNIGHT, 2004).

Na mesma PDD-39, em seu item 4, letra "d", salta aos olhos a atribuição designada para a Federal Emergency Management Agency (FEMA), na medida em que é determinada a responsabilidade da referida agência pela adequação de planos de resposta a incidentes terroristas. Na sequência veio a edição da PDD-62, em 22 de maio de 1998, e, mais tarde, seis semanas após os atentados de 11 de setembro, foi decretado o Ato Patriótico, em 26 de outubro de 2001, que mudou consideravelmente o rosto do antiterrorismo nos EUA, sobretudo em atribuir responsabilidades ao FBI.

Diante das dificuldades encontradas em gerenciar o atentado de 11 de setembro de 2001, o então presidente dos EUA, George W. Bush, editou a *Homeland Security Presidential Directive* 5 (HSPD-5), em 28 de março de 2003, cujo principal propósito foi estabelecer um único sistema de gerenciamento de incidentes de âmbito nacional. Em seu bojo, a norma ampliou as atribuições da *Secretary of Homeland Security*, incumbindo-a de desenvolver, aplicar, certificar e auditar o *National Incident Management System* (NIMS), que passou a normatizar todo o ciclo de gerenciamento de qualquer incidente nos EUA, para os governos federal, estadual e municipal, bem como para organizações não governamentais (ONG) e o setor privado.

Essa modificação envolveu toda a sociedade em um esforço de trabalho conjunto, tudo isso amparado por uma terminologia e uma doutrina comuns, com o objetivo de prevenir, proteger, responder, recuperar e mitigar os efeitos dos incidentes, independentemente de causa, tamanho, localização ou complexidade.

> Para fornecer interoperabilidade e compatibilidade entre os recursos federais, estaduais e locais, o NIMS incluirá um conjunto básico de conceitos, princípios, terminologia e tecnologias que cobrem o Sistema de Comando de Incidente; sistemas de coordenação multiagências; comando unificado; treinamento; identificação e gerenciamento de recursos (incluindo sistemas para classificação de tipos de recursos); qualificações e certificação; e a coleta, o rastreamento e o relatório de incidentes, informações e recursos de incidentes. (ESTADOS UNIDOS DA AMÉRICA, 2003, p. 229, tradução nossa).

Por ser um órgão federal, o FBI se adequou a essa nova terminologia comum do NIMS, não podendo ficar alheio às mudanças diante do novo e complexo Sistema Nacional de Gestão de Incidentes. Importante destacar que o termo "complexo", aqui utilizado, surge como sinônimo de integrado, e não como algo dificultoso. Essa adequação também pode ser percebida quando integrantes da referida instituição federal ministraram um curso no Brasil, em 2 de maio de 2012, e utilizaram o termo "incidente" no lugar de "crise", definindo-o como: "[...] uma ocorrência causada ou pelo ser humano ou por um fenômeno natural, que exige resposta imediata".[1]

Mais de quinze anos depois, em 10 de outubro de 2017, a FEMA publicou a terceira edição do NIMS 2017, sedimentando a sua doutrina, ao definir o termo "incidente", em seu glossário, como:

> Incidente: Uma ocorrência, natural ou provocada pelo homem, que requer uma resposta para proteger a vida ou a propriedade. Neste documento, a palavra 'incidente' inclui eventos planejados, bem como emergências e/ou desastres de todos os tipos e tamanhos. (ESTADOS UNIDOS DA AMÉRICA, 2017, p. 64, tradução nossa).

Contudo, ao pesquisar as normas de gerenciamento de incidentes, ainda é possível encontrar o FBI utilizando o termo "crises". Um exemplo disso pode ser encontrado no Plano de Resposta Nacional de 2004 (NRP, na sigla em inglês), e no seu anexo sobre *Terrorism Incident Law Enforcement and Investigation*. Infere-se, desses textos, editados em 2004, mas ainda vigentes, que o órgão federal utilizou o termo "crises" enquanto evento extraordinário, crucial. Ao que tudo indica, o motivo foi a falta de atualização e de revisão do anexo do NRP.

Por seu turno, no estado de São Paulo, o Sistema Integrado de Comando e Operações em Emergências (SiCOE), regido pela Diretriz nº CCB-004/931/2014, apesar de citar, em seu texto, o termo "incidentes" em diversas passagens, não o define. Todavia, em seu glossário, é possível identificar a opção pelo termo "emergência" como sinônimo. Nessa mesma norma, é asseverada a adequação do *Incident Command System* (ICS) para a gestão de emergências no estado de São Paulo e no Brasil, conforme o item 2, letra "c":

> [...] c. O *Incident Command System (*ICS), desenvolvido pelo gestor de serviço de bombeiros do Estado da Califórnia, EUA, nos anos 70, foi adotado como padrão pelo Federal Emergency Management Agency (FEMA - USA) e pela Secretaria Nacional de Segurança Pública (SENASP - Brasil) e se mostra adequado para a gestão de emergências no Estado de São Paulo e no Brasil, uma vez que vem sendo metodicamente adaptado pelas forças de segurança do país com os nomes de Sistema de Comando em Operações (SCO) e Sistema de Comando em Incidentes (SCI). (CORPO DE BOMBEIROS DA POLÍCIA MILITAR DO ESTADO DE SÃO PAULO, 2014).

Vale dizer que o ICS se subordina aos conceitos do NIMS e, assim, respeita o princípio da terminologia comum. Esse procedimento oferece um ambiente apto para que diversas organizações de gerenciamento de incidentes e de suporte possam trabalhar em conjunto, evitando, desse modo, confusões e perda de tempo com termos e nomenclaturas durante um incidente:

> O NIMS orienta todos os níveis de governo, organizações não governamentais (ONG) e o setor privado a trabalharem juntos para prevenir, mitigar, responder, recuperar e proteger contra incidentes. O NIMS oferece aos interessados em toda a comunidade o vocabulário, os sistemas e os processos compartilhados para fornecer com sucesso os recursos. descritos no Sistema Nacional de Preparação. **O NIMS define sistemas operacionais, incluindo o Sistema de Comando de Incidente (ICS)**, as estruturas do Centro de Operações de

[1] Definição obtida diretamente no Curso de Pronto Atendimento e Investigações em Incidentes com Agentes Químicos, Bacteriológicos, Radiológicos e Nucleares, ministrado pelo FBI, em São Paulo, em 2 de maio de 2012, durante a sétima aula (*Incident Management – Command and Control* – ICS).

> Emergência (EOC) e os Grupos de Coordenação Multiagências (Grupos MAC) que orientam a forma como o pessoal trabalha em conjunto durante os incidentes. O NIMS aplica-se a todos os incidentes, de acidentes de trânsito a grandes desastres. (ESTADOS UNIDOS DA AMÉRICA, 2017, p. 1, tradução e grifo nossos).

Seja como for, a opção pelo termo "incidente" ou "emergência" e a sua definição são importantes, pois repercutem no âmbito do Direito, uma vez que o termo "Comandante do Incidente" define a extensão de seus deveres e de suas obrigações na função. Nesse sentido, se utilizada a definição de incidente, em muito se expande o poder-dever de atuação dos órgãos, devido à sua maior carga preventiva.

Prefere-se o termo "incidente", definido acima, no lugar de "crise" e de "emergência", a fim de acompanhar a melhor doutrina de Gerenciamento de Incidentes, na toada do NIMS 2017, bem como de seguir a vocação preventiva da Polícia Militar do Estado de São Paulo (PMESP). A Tabela 1 apresenta as características do NIMS.

Tabela 1 - Visão geral do NIMS.

NIMS é	NIMS não é
● Uma abordagem abrangente, em todo o país, sistemática para o gerenciamento de incidentes, incluindo o comando e a coordenação de incidentes, o gerenciamento de recursos e o gerenciamento de informações.	● Somente o ICS. ● Único sistema aplicável a certos funcionários de resposta de emergência/incidente. ● Um sistema estático.
● Um conjunto de conceitos e princípios para todas as ameaças, perigos e eventos em todas as áreas da missão (Prevenção, Proteção, Mitigação, Resposta e Recuperação).	● Um plano de resposta.
● Escalável, flexível e adaptável; usado para todos os incidentes, desde o dia a dia até a grande escala.	● Usado somente durante incidentes em grande escala.
● Um conjunto de procedimentos padrão de gerenciamento de recursos, que permite a coordenação entre diferentes jurisdições ou organizações.	● Um sistema de pedidos de recursos.
● Um conjunto de princípios essenciais para a comunicação e o gerenciamento de informações.	● Um plano de comunicação.

Fonte: Estados Unidos da América (2017, p. 2), adaptado de NIMS 2017.

Nota: Para que se possa compreender a sua grandiosidade, é relevante destacar que o NIMS define os sistemas operacionais nos EUA, incluindo o Sistema de Comando de Incidente.

Convém mencionar que a obra de Scachetti Júnior (2014) versou sobre o seguinte tema: *Sistema de Comando e Controle: análise conceitual e perspectiva de utilização conjunta pela Polícia Militar, Corpo de Bombeiros e Defesa Civil do estado de São Paulo*. Em seu notável estudo, é possível localizar uma análise precisa que merece ser transcrita:

> Diante do exposto, torna-se nítida a necessidade e importância da utilização de um sistema de C2 unificado e padronizado no Estado de São Paulo que proporcione a melhoria do atendimento e gerenciamento das emergências, de forma isolada ou integrada, pela Polícia Militar, Corpo de Bombeiros e Defesa Civil. Por tudo o que foi apresentado e levando-se em conta fatores como requisitos, foco de atuação, maturidade e tempo de desenvolvimento, sugere-se pela adoção e padronização do SiCOE do CBPMESP como sistema único também para a PMESP e a Defesa Civil de São Paulo. Essa medida não tem o intuito de apontar ou classificar os sistemas de C2 um como melhor que o outro, mas prioriza um padrão em razão de sua aceitabilidade e aplicabilidade, de maneira que a disseminação do conhecimento possa ser efetiva. Essa padronização traria grandes vantagens, pois alinharia os principais órgãos de primeiro atendimento a emergências do Estado de São Paulo (PMESP, CBPMESP e Defesa Civil), relativamente à terminologia e doutrina, facilitando a organização e o desenvolvimento dos trabalhos de forma colaborativa e integrada, otimizando a tomada de decisões e o gerenciamento dos recursos disponíveis, bem como potencializando em muito os trabalhos em ambiente interagências. Além disso, os seus agentes estariam sendo preparados dentro de um sistema internacionalmente reconhecido, independente da designação, com plena capacidade de representar o Estado de São Paulo em quaisquer circunstâncias ou eventos que venham participar em apoio. (SCACHETTI JÚNIOR, 2014, p. 135-136, grifo nosso).

A conclusão é perfeita, cabendo acrescentar que o ICS e o SiCOE são ferramentas de atendimento operacional de um incidente em camada local, enquanto o NIMS é muito mais ambicioso do que isso, pois define atribuições para o problema em *layer* (camada) acima do nível local do incidente, vocacionando-se para a gestão político-estratégica de apoio.

É interessante notar que, no Brasil, as ocorrências policiais mantiveram-se distantes de serem gerenciadas segundo a metodologia do ICS/SiCOE. O mesmo ocorreu nos EUA, onde a

própria origem do conceito do ICS começou por conta de incêndios florestais, em 1970, com o sistema chamado *Firefighting Resources of Southern California Organized for Potential Emergencies* (FIRESCOPE), sendo que somente a partir de 1984 é que se iniciaram os estudos para a aplicação do ICS aos diversos incidentes policiais[2], independentemente de causa, tamanho, complexidade e localização, destacando-se como pioneiro nesse trabalho o *San Bernardino County Sheriff's Department*, na Califórnia.

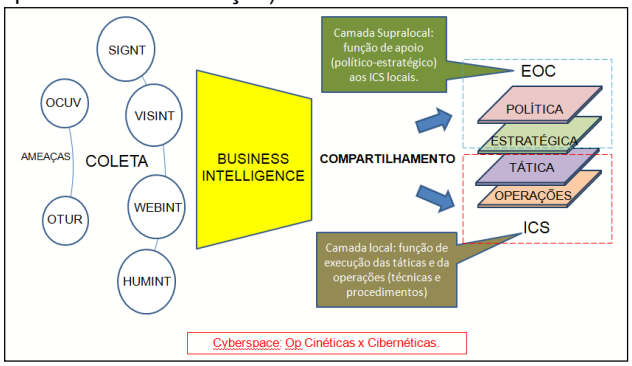
Deseja-se que a filosofia do NIMS 2017 seja utilizada para o gerenciamento de todos os tipos de incidentes, principalmente os policiais, dos mais simples aos mais complexos, utilizando-se, em nível local, a estrutura do ICS/SiCOE, já consolidada pelo Corpo de Bombeiros, mas incorporando-se o conceito de *Emergency Operation Center* (EOC), função essa político-estratégica em camada superior ao local do incidente e de apoio a ele.

Em linhas gerais, o EOC é uma arquitetura retratada no NIMS 2017, podendo funcionar 24/7 e ser utilizada como ICS emergencial, até que se estabeleça uma estrutura no local da ocorrência. Mas a grande vocação desse tipo de centro é o gerenciamento político-estratégico em apoio a uma ou a múltiplas estruturas de ICS que estejam mobiliadas em diferentes regiões geográficas simultaneamente. Ou seja, gerenciamento de incidentes múltiplos e complexos.

Em São Paulo, o Centro de Operações da Polícia Militar (COPOM) é vocacionado para o registro de ocorrências, entretanto, é certo que se afigura como local ideal para hospedar o conceito de EOC com tecnologia de Comando, Controle, Comunicações, Computadores, *Cyber* e Inteligência (C5I) e hipertrofiar sua capacidade de gerenciamento de incidentes, concebendo consciência situacional e compartilhamento de imagem operacional comum com ultravelocidade, ferramentas essas fundamentais para o processo decisório efetivo (

Figura 1).

Figura 1 - Processo de coleta, análise e compartilhamento de informações e de Inteligência: dicotomia entre o EOC (nível político-estratégico de apoio) e o ICS (tático-operacional de execução).



Fonte: Elaborada pelo autor (2017).
Legenda: Inteligência dos Sinais (SIGNT), Inteligência Visual (VISINT), Inteligência de Web (WEBINT), Inteligência Humana (HUMINT), Organizações Criminosas Ultraviolentas (OCUV) e Organizações Terroristas Ultrarradicais OTUR).

2 CONSEQUÊNCIAS DO ALARGAMENTO DO CONCEITO DE CRISES E ADOÇÃO DO TERMO"INCIDENTE"

Inicialmente, é importante resgatar a análise comparativa de Aguilar *et al*. (2017, p. 4) contrapondo o significado de "incidente", utilizado no NIMS 2017, à expressão "crises", usada pela Academia do FBI e trazida ao Brasil em meados da década de 1990:

> Destarte, a definição de incidente utilizada no NIMS 2017 difere da utilizada pela Academia do FBI, na década de 90, em dois pontos principalmente: 1) inclui não apenas crises, mas qualquer evento que denote possibilidade de perigo de lesão à vida ou ao patrimônio, inclusive eventos planejados, como manifestações públicas e eventos esportivos, que são incidentes que podem evoluir para crises; 2) silencia quanto ao órgão responsável pelo incidente, não sendo a polícia a única responsável durante a *timeline* de um incidente, que pode variar em tamanho e complexidade, exigindo a participação e responsabilidades de outros órgãos vocacionados para o incidente e até mesmo de outras esferas do governo, ONG e setor privado, uma vez que o objetivo final é a Prevenção, Preparação, Mitigação, Resposta e Recuperação.

A definição de "incidente" utilizada no NIMS 2017 possui carga preventiva superior ao termo "crise", no tocante aos bens jurídicos tutelados. Isso porque, ao incluir o verbo "proteger", envereda-se pela manutenção da ordem pública, em todo o seu espectro, definição essa que se amolda às funções constitucionais da PMESP e às Normas para o Sistema Operacional de Policiamento PM (NORSOP) (POLÍCIA MILITAR DO ESTADO DE SÃO PAULO, 2006).

Duas são as principais consequências do alargamento do termo "crise": 1) deve-se gerenciar o incidente, o quanto antes, em seus estágios iniciais, para que ele não evolua para uma crise, de modo que a velocidade de resposta ganhe prioridade; 2) o gerenciamento de incidentes passa a ser uma resposta do estado com a participação da sociedade, incentivando-se o princípio do comando unificado,

[2] Incidentes policiais são caracterizados pelo conflito de interesses entre a polícia e o suspeito. Justamente por isso, são considerados os incidentes mais perigosos.

pelo qual várias instituições e organizações com competências técnicas ou legais sobre o incidente estabelecem um conjunto de objetivos e de estratégias comuns, consubstanciado no Plano de Ação do Incidente (PAI). Cumpre observar que, embora essas decisões sejam conjuntas, deverá ser designado um único comandante/responsável, pertencente à instituição com maior pertinência técnica ou legal sobre o incidente.

Cabe lembrar que a PMESP possui, em sua estrutura,12 magníficos Centros de Fusão de Informações: o Centro de Inteligência da Polícia Militar (CIPM) e os 11 Centros de Operações da Polícia Militar (COPOMs), capilarizados 24/7 em todos os municípios do estado, afigurando-se como a instituição com a maior capacidade operativa para hospedar um comando unificado dotado de significativa tecnologia C5I quando em cenários caóticos, seja em nível local de ICS ou em camada supralocal em um EOC. Apesar disso, nem sempre terá como Comandante do Incidente um oficial da polícia militar. Esses casos, em que a pertinência principal não seja da PMESP, serão resolvidos por meio de designação pelos secretários de Estado ou pelo governador, uma vez serem incidentes que envolvem competências, pastas e alocação de recursos de secretarias diferentes.

2.1 A Quarta Revolução Industrial e a Polícia Militar do Estado de São Paulo

É válido considerar que a instituição bandeirante se esforça para realizar a preservação da ordem pública em seu mais amplo aspecto de prevenção, acompanhando, prematuramente, incidentes potencialmente lesivos à vida, à propriedade, ao meio ambiente e à informação, antes mesmo de haver a quebra da ordem pública, executando, assim, o estado da arte em prevenção. Exemplos disso são o policiamento ostensivo inteligente e o acompanhamento de manifestações públicas pacíficas, previamente comunicadas às autoridades, bem como de eventos esportivos ou culturais de porte considerável, ou mesmo o sofisticado policiamento ambiental realizado por meio de veículo aéreo não tripulável (VANT).

Minuto a minuto, de forma sorrateira, somos seduzidos pela Quarta Revolução Industrial ou Indústria 4.0, marcada, sobretudo, pela Internet das Coisas (*Internet of Things – IoT*), pelo aprendizado de máquina (*machine learning)* e pela computação em nuvem (*cloud computing*). Pouco a pouco, nos tornamos, de uma forma ou de outra, usuários de *Big Data Analytics*, de Mineração de Dados (*Data Mining*) e de Inteligência de Negócios (*Business Intelligence*), posto que vivemos em uma era de transformação do mundo físico para o mundo digital. E essa inflexão será intensificada nos próximos anos, com o advento das Cidades Inteligentes (*Smart Cities*).

Nesse contexto, Calegari (2017) explica que o estado de São Paulo é, de longe, a unidade da Federação com o maior número de cidades inteligentes, contando com 46 municípios entre os 100 primeiros, dentre os quais se destaca a cidade de São Paulo, que ocupa o topo, como município mais inteligente e conectado do Brasil, segundo aponta o *ranking Connected Smart Cities 2017*.

Os problemas urbanos também se intensificaram em decorrência da Quarta Revolução Industrial, que se afigura como substância catalisadora de cenários VUCA. Cunhado na década de 1990 pelo *U.S. Army War College*, o termo VUCA é utilizado para descrever cenários caracterizados por volatilidade (*volatility*), incerteza (*uncertainty*), complexidade (*complexity*) e ambiguidade (*ambiguity*). Grosso modo, VUCA é o caos, cabendo à Polícia Militar entendê-lo e gerenciá-lo, a fim de minimizar seus efeitos disruptivos.

Como consequência desses novos cenários, os incidentes tornaram-se liquefeitos, exigindo que a polícia militar aumente a sua capacidade operativa, estimulando as suas ações de fiscalização de polícia e, por vezes, de restauração da ordem pública. Felizmente, toda essa tecnologia e a inovação propiciada pela Indústria 4.0 também vêm ao socorro do estado, no sentido de potencializar a sua capacidade responsiva, incluindo-se, aqui, respostas diante de incidentes de todos os tamanhos, causas, localizações e complexidades.

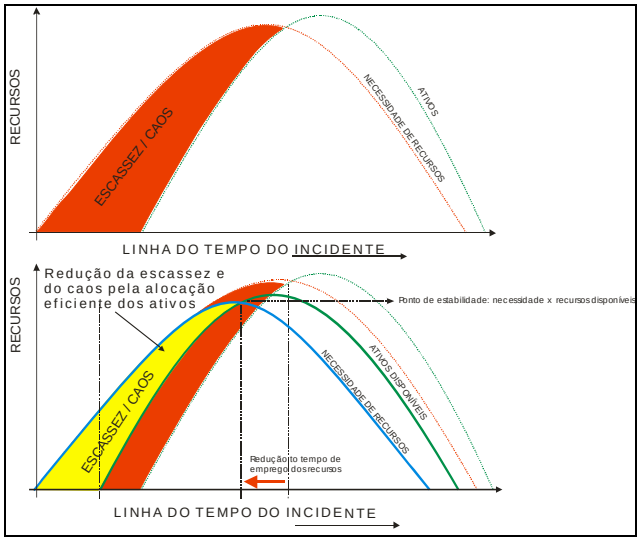
No início dos anos de 1990, qual era a capacidade computacional do policial militar ao assumir o serviço de policiamento ostensivo motorizado? Recordo-me que, ao assumir o serviço, eram obrigatórios: a prancheta com a lista dos últimos veículos roubados ou furtados (lista de caráter geral), o telefone celular analógico, o guia de ruas impresso e, claro, o rádio da viatura. Era o que existia! E hoje? Hoje, temos os *smartphones*, que superam em muito a capacidade de processamento de computadores tradicionais, dotados com aplicativos para quase tudo, inclusive com guia de endereços, fluxo de trânsito, consulta de placas de veículos etc. Além disso, temos também a rede 4G, os aplicativos BOPM Eletrônico e Termo Circunstanciado, o *Big Data* do COPOM on-line, o Projeto Radar, com *insights* em tempo real dos veículos roubados e furtados detectados, que aparecem automaticamente nos *tablets* das viaturas por meio de *pop-up*, dentre outras utilidades.

Sem dúvida, a capacidade computacional do policial militar cresceu exponencialmente nos últimos vinte anos. Quadros brancos e*flipcharts* funcionam muito bem para expor informações em cenários de gerenciamento de incidentes ou em Postos de Comando (PCs), isso é verdade! Concorda-se! Entretanto, são limitados em Inteligência Visual e desprovidos de capacidade computacional de mineração de dados (*data mining*) e de análise de vínculos (AV), de forma que são muito bem-vindos como ferramentas de apoio inicial, ou como meios auxiliares, até que uma infraestrutura computacional seja implementada, sendo certo que essa estrutura dependerá do tamanho e da duração do evento, estabelecendo-se conforme o efeito *leggo*, pelo qual a estrutura de recursos mobilizados vai aumentando segundo as necessidades.

Ocorrendo incidentes complexos em

diferentes áreas geográficas de forma simultânea, como ataques múltiplos e coordenados, *Multi-Assault Counter-Terrorist Action Capabilities* (MACTAC), ou Capacidade de Resposta Contraterrorista Frente a Múltiplos Ataques (AGUILAR, 2016), presídios rebelados, incêndios de grande porte ou epidemias, todos esses eventos são classificados como crises de grande demanda, porque requerem grande quantidade de coleta, análise, processamento e compartilhamento em ultravelocidade de informações e de Inteligência, para que possam ser alocados, tão rapidamente quanto possível, os ativos operacionais necessários, sem excesso de recursos em um primeiro incidente e escassez em uma onda de ataques subsequentes, e para que se possa descobrir a causa e a natureza dos eventos, evitando-se o escalonamento do incidente ou impedindo que novos ataques ocorram (Figura 2).

Figura 2 - Antecipando necessidades de recursos nos incidentes



Fonte: Estados Unidos da América (2013, p. 9), módulo 6, FEMA – IS-0200.B.

Nesse cenário, faz todo o sentido essa tecnologia, a fim de propiciar que o ciclo decisório se retroalimente com ultravelocidadede, dados cada vez mais minerados (*data mining*) e vinculados (AV), respeitando os requisitos 5V: v**olume**, v**ariedade** e v**elocidade** (aspectos quantitativos dos dados), veracidade (aspecto qualitativo) e valor (aspecto de vantajosidade), resultando em decisões mais rápidas, adaptadas e eficientes, reduzindo-se o tempo de resposta.

Cumpre consignar que a PMESP não está alheia à Quarta Revolução Industrial. De forma relevante, a instituição insere-se nesse contexto por meio de diversos sensores cibernéticos, a cada chamada recebida pelo telefone 190, perfazendo 40 mil ligações diárias; a cada *login* de computador embarcado, quando uma patrulha assume o turno de serviço; pelo rastro digital, deixado pelo caminho da viatura policial por onde passou; pela geolocalização de cada policial militar, ao usar o *Global Positioning System* (GPS); pelos *tablets*; pelos Terminais Móveis de Dados (TMDs); pelos Terminais Portáteis de Dados (TPDs); pelas câmeras inteligentes fixas e corporais (*body-worn câmeras – BWCs*) etc. Tudo isso interligado a uma rede de aplicativos complexos, no sentido de integrados: Sistema Interno de Ocorrências Policial Militar (SIOPM), COPOM on-line, Informações Criminais (Infocrim), dentre outros.

Merecem destaque, também, os megaprojetos da PMESP, o Boletim de Ocorrência Eletrônico (BOe) e o Termo Circunstanciado de Ocorrência Eletrônico (TCOe), que trazem extraordinária eficiência ao serviço de polícia ostensiva para a população, porque capacitam os policiais militares a realizarem a escrituração dos crimes de menor potencial ofensivo, resolvendo a ocorrência do cidadão no local dos fatos, sem necessidade de deslocamento para as Delegacias. Tudo digital! E o mais importante: tudo integrado!

Todos esses sensores e aplicativos geram extraordinárias quantidades de dados digitais e de comunicações sobre segurança pública que facilmente são obscurecidos pelo volume, e que, por isso, devem ser minerados, extraindo-se vínculos e análises preditivas, tornando mais ágil, adaptável e eficiente a capacidade de resposta em gerenciar incidentes.

Os sensores cibernéticos da Indústria 4.0 são compostos por dispositivos computacionais conectados em rede ou não, que armazenam e processam informações, disparando *insights* em tempo real, provocando a digitalização do incidente em painéis analíticos dispostos em camadas, como mapas de análises de vínculo i-2, georreferenciamento, biometria de suspeitos envolvidos (incluindo-se digitais, DNA, reconhecimento facial etc.), além de metas, métricas e indicadores de desempenho do incidente nos aspectos de planejamento, operações, finanças, logística e Inteligência. Todos esses dados devem estar dispostos de forma *friendly* (amigável) para os comandantes do incidente, ou seja, em formato de infográficos, capazes de exibir essas informações de várias maneiras, por ordem cronológica, grau hierárquico, grau de risco, prioridade de atendimento, desempenho, ou até mesmo organizando-as segundo outros perfis designados por grupos ou por elementos-chave, gerando *insights personalizados*.

Incidentes liquefeitos, confusos, imprevisíveis, que se metamorfoseiam com velocidade, exigem, como nunca, que os dados sejam iluminados para os decisores por meio de conceitos de *Inteligência Visual* ou de *Data Storytelling*.[3]

Na maioria das vezes, o comandante do incidente ou as autoridades corresponsáveis do comando unificado não são profissionais de

[3] *Data Storytelling* é o resultado do que chamamos de pacote completo: uma solução que seja capaz de analisar dados, cruzá-los e ainda dispor de uma interface que possibilite a construção de apresentações visuais. Com isso, os tomadores de decisão conseguem utilizar apenas uma plataforma para entender o cenário, fazer análises preditivas e apresentar as informações com embasamento e praticidade (GUERRA, 2016).

Tecnologia da Informação e Comunicação (TIC), mas expertos no incidente. Em consequência disso, de nada adiantará especialistas designados para um determinado incidente, se não lhes for disponibilizado o entendimento visual para que possam enxergar o valor do que está sendo mostrado, de forma a lhes permitir usufruírem de *insights* em tempo real. Privilegia-se a visualização a meros números.

Justamente por isso existe a necessidade de as salas de C5I terem painéis eletrônicos ou telões (Figura 3). Entretanto, observa-se que esses painéis não devem ser utilizados apenas para transmitir imagens de câmeras a respeito de uma ocorrência em andamento, funcionando como mera televisão gigante, mas, principalmente, devem ser utilizados para transmitir a visualização analítica de dados e de Inteligência produzida a respeito de um incidente.

Figura 3 - Centro de Operações da Polícia Militar do Estado de São Paulo

Fonte: **A3PM - Agência de Publicidade e Propaganda da Polícia Militar, Centro de Comunicação Social da PMESP (2017)**.

Few (2004) discorre com propriedade acerca da Inteligência Visual:

> Algumas das oportunidades mais interessantes para *business intelligence* hoje podem ser vislumbradas em tecnologias que estão apenas começando a explorar o incrível potencial da visualização de informações. Nem todas as informações se prestam aos mesmos meios de análise e apresentação. Às vezes, a descoberta eficaz envolve a leitura de pilhas de documentos de texto ou o estudo laborioso de fileira após fileira de detalhes em relatórios tabulares, mas, muitas vezes, nossos maiores *insights* surgem quando analisamos fotos de dados. A visão é o nosso sentido dominante. Ao examinar uma visualização de dados adequadamente projetada, às vezes, experimentamos um *flash* de reconhecimento, que, de outra forma, levaria horas de doloroso estudo para descobrir. Um computador apresenta uma representação visual, permitindo-nos manipular a exibição de várias maneiras para desvendar o seu significado. Gráficos estáticos, embora úteis, não são um exemplo de visualização de informações. Mas se você representar graficamente informações abstratas em uma tela de computador de uma maneira que permita a exploração através da manipulação dinâmica da exibição (filtragem, realce, reorganização e assim por diante), resultando na descoberta de significado, você estará envolvido na visualização da informação. Faça bem e os *insights* resultantes podem ser extraordinários. (FEW, 2004, tradução nossa).

2.2 Centros de Fusão no estado de São Paulo

Nessa linha de raciocínio, o COPOM ganha total relevância, pois, além de possuir vocação para alojar um EOC com tecnologia C5I, é o primeiro órgão a perceber e a responder com agilidade e resiliência, em tempo real, a incidentes de todas as ameaças e tamanhos. Sua capacidade responsiva lhe é própria, visto que domina ativos operacionais dotados do conceito *boots on the ground* (botas no chão), atuando 24/7 em todos os municípios do estado de São Paulo. Já a sua capacidade de perceber incidentes em tempo real decorre dos *ativos cinéticos* representados pelos policiais dispostos no terreno e dos *ativos cibernéticos* (sensores cibernéticos) exemplificados acima.

Todos esses sensores trazem *input* de dados, propiciando a percepção do incidente em seus momentos iniciais. Na sequência, o COPOM os devolve em *output*, por meio do gerenciamento de incidente, designando os ativos operacionais, a fim de atender incidentes dos mais simples aos mais complexos. Quanto mais rápida essa mobilização de ativos operacionais para o problema, mais rápido o incidente será estabilizado, e, em consequência disso, mais vidas serão salvas, conforme o ponto de estabilidade da Figura 2.

Certamente, as equipes do policiamento territorial (190) são as primeiras respondedoras de qualquer incidente e, por isso, ganham destaque na Indústria 4.0, na medida em que suportam as consequências da necessidade de priorizar um ciclo decisório que deve ser extremamente rápido e resiliente ao problema. É necessário sempre ter em mente que o primeiro policial que chega ao local da ocorrência assume as funções de Comandante do Incidente Emergencial, até que ocorra a chegada de outras autoridades responsáveis, momento em que se dará a transferência de comando e o escalonamento da resposta, efeito *leggo.*

É imprescindível destacar que a proteção prematura de incidentes favorece duas ferramentas fundamentais em processo decisório: a Consciência Situacional (CS) e a Imagem Operacional Comum (IOC). Heal (2002, p. 43, tradução nossa), um dos

maiores estrategistas de segurança pública nos EUA, explica ambos os instrumentos precisamente:

> A consciência situacional é um conceito que descreve o conhecimento e a compreensão de uma pessoa sobre as circunstâncias, os ambientes e as influências em relação aos desdobramentos de uma situação. Imagem Operacional Comum é simplesmente o conhecimento e a compreensão compartilhados entre indivíduos, equipes ou grupos. Embora de natureza semelhante, a Consciência Situacional e a Imagem Operacional Comum são diferentes em muitos aspectos. Por exemplo, a consciência situacional pertence a um indivíduo, enquanto uma imagem operacional comum, por definição, pertence a um grupo. Isso tem duas implicações. Primeiro, cada uma serve a um propósito. A consciência situacional destina-se a fornecer a um indivíduo uma visão e uma descrição, enquanto uma imagem operacional comum cria compreensão compartilhada para aprimorar a colaboração e criar sinergia.

Ou seja, a consciência situacional é uma ferramenta mais destinada ao Comandante do Incidente e à concepção individual dos respondedores, enquanto a imagem operacional comum destina-se a compartilhar o entendimento do incidente em ambiente interagências e nos diversos níveis hierárquicos. Quando utilizadas em conjunto, provocam um significativo efeito sinergético, impulsionado pela imagem operacional comum, o que favorece ao entendimento compartilhado de ameaças e de oportunidades entre os diversos níveis hierárquicos (compartilhamento vertical) e entre os vários órgãos responsáveis pelo incidente (compartilhamento horizontal), trazendo hipervigilância do incidente em tempo real:

> Uma imagem operacional comum, por outro lado, fornece um quadro de referência que uma organização precisa para alcançar uma coordenação e colaboração eficazes e eficientes. As metas e os objetivos são mais facilmente percebidos e mais fáceis de concordar, enquanto as prioridades são menos propensas a serem controversas. As oportunidades e as ameaças são mais facilmente discernidas porque o entendimento comum cria uma vigilância compartilhada através de todos os componentes organizacionais e níveis de comando. Todo o processo de tomada de decisão, de fato, torna-se sinérgico porque cada componente ou escalão é capaz de compreender e contribuir de acordo com o entendimento comum. Parece razoável que, quanto maior a consciência situacional, e quanto mais comum o quadro operacional comum, mais provável que as decisões sejam efetivas e a organização funcionará sem problemas e de forma mais eficiente. (HEAL, 2002, p. 43, tradução nossa).

Organizações Criminosas Ultraviolentas e Organizações Terroristas Ultrarradicais, estruturadas em pequenos grupos, muitos sem uma liderança definida, e que se utilizam de comunicação em tempo real, encontram em ambientes VUCA condições ideais de sucesso.

O general McChrystal (2015), no livro *Team of teams*, elucida que, para se combater tais organizações, nesses cenários, é fundamental que se tenha consciência compartilhada, com ultravelocidade nas comunicações (o que, neste texto, é chamado de imagem operacional comum), mas adverte que isso não é suficiente, sendo crucial que também ocorra o deslocamento do poder decisório para níveis hierarquicamente inferiores, descentralizando-se as ações em campo, a fim de se agilizar a capacidade de resposta e de resiliência. Busca-se evitar que a decisão tenha que percorrer vários escalões de C2 (Comando e Controle), como em estruturas *top down* ou piramidais, ocasionando lentidão nas ações, gerando-se respostas inoportunas diante de situações-problema fluidas que já evoluíram.

Dessa forma, os policiais que possuem as *botas no chão* devem ser *empoderados* na execução das missões em campo, de tal sorte que possam atuar como células semiautônomas, o que lhes permite buscar, criar e explorar oportunidades com base em sua consciência situacional individual gerada por toda essa tecnologia. Deseja-se que as equipes policiais em campo respondam e se adaptem em meio a cenários caóticos com mais agilidade e precisão se comparados com estruturas tradicionais de C2 (*top down*).

Ainda nas lições do general, a eficiência, não obstante ser extremante necessária, deixou de ser suficiente para o sucesso, ganhando prioridade a capacidade de responder e de se adaptar rapidamente diante de cenários VUCA (MCCHRYSTAL, 2015). Nesse sentido, é acertada e imprescindível a atuação de um Comandante Emergencial, que responda ao incidente com extrema agilidade, mas a título precário, até que um Comandante Efetivo se apresente com os meios mais eficientes e disponíveis para o incidente.

A grande armadilha da Quarta Revolução Industrial, marcada com tecnologias e salas de C5I, é que as autoridades do alto escalão, imbuídas e beneficiadas pela hipervigilância, acreditem e desejem comandar e controlar cada passo do policial que está no campo de ações, em meio ao caos. A cúpula tem de afastar-se do papel de centralização da autoridade decisória e tornar-se um elemento facilitador do processo, para que as equipes em campo tenham sucesso, exercendo a função de apoio ao Comandante do Incidente, que está no local realizando a execução das operações. Exemplo disso são as estruturas de EOC, que, por meio de decisões

político-estratégicas, apoiam o ICS em camada local.

Vale notar que, em junho de 2018, o Comando-Geral da PMESP criou o Estágio de Atualização em Liderança Operacional, cuja abrangência compreende 12 mil policiais militares. O estágio segue a dogmática moderna, pois muda a prioridade do foco na eficiência para a capacidade de resposta/resiliência, bem como desloca o poder decisório para níveis inferiores de andamento, *empoderando a* função do Comandante de Grupo de Patrulha.

Sem dúvida, para a implementação efetiva desses novos horizontes dogmáticos, marcadamente em instituições piramidais mais conservadoras, será necessária uma mudança de estruturas, de processos e, principalmente, de mentalidade, por meio de um esforço sustentado por parte da liderança, a fim de se fomentar e criar um ambiente propício para que tais mudanças ocorram.

2.3 Inteligência como protagonista do Ciclo OODA no gerenciamento de incidentes

A Inteligência ganha especial destaque no Ciclo Observar, Orientar, Decidir e Agir (OODA), para tornar os ciclos decisórios mais ágeis, sendo representada pela fase de orientação (análise, compartilhamento e assessoramento). Trata-se da última estrutura do ciclo, capaz de ser organizada previamente e mantida permanentemente 24/7, uma vez que a próxima fase, a decisória, é representada pelo Comandante do Incidente Emergencial ou Efetivo.

As informações e as análises devem estar disponíveis, aquecidas, retroalimentadas e em formato amigável, para se tornarem imediatamente disponíveis e utilizáveis pelo Comandante Emergencial, resultando em respostas ágeis e adaptadas frente ao incidente que se apresenta e que evolui. Ocorre que nunca saberemos ao certo qual espécie de incidente eclodirá, logo, nunca saberemos quais serão os requisitos exigidos para se designar um Comandante do Incidente Efetivo vocacionado para o evento. O próximo incidente exigirá conhecimentos de bombeiro? De policiamento de trânsito? De policiamento rodoviário? De ações táticas? De operações especiais? De saúde? De assistência social? Impossível saber. E é justamente por isso que a Inteligência funciona como sentinela de dados e análises.

No intuito de agilizar a tomada de decisão e de centralizar os dados e as informações, recomenda-se a utilização de *softwares aplicativos* de Comando e Controle, com capacidade de *gerar consciência situacional, distribuir imagem operacional comum e sincronizar as ações* dos ativos mobiliados em campo, além de controlar aspectos de planejamento, operações, finanças, logística e Inteligência do incidente em tempo real (Figura 4). Como consequência, será possível que um EOC com capacidade C5I consiga digitalizar cenários de incidentes múltiplos, simultâneos e complexos. Por exemplo, será possível acompanhar três grandes manifestações em diferentes pontos do estado de São Paulo, contando cada uma com pelo menos 10 mil pessoas; ou três grandes roubos a sedes de transporte de valores, com 20 marginais fortemente armados em cada um; ou três incêndios de grande magnitude; ou até mesmo digitalizar e acompanhar todos esses incidentes ao mesmo tempo, em painéis analíticos, no formato de infográficos e de imagens dos fatos.

Figura 4 - Exemplo de Matriz de Sincronização de Ações do *software* aplicativo Pacificador, utilizado pelo Exército Brasileiro

Fonte: Kohl (2013).

Nota: Uma das telas mais importantes em qualquer programa de C2 é a Matriz de Sincronização de Ações. A Inteligência Visual permite, no caso da figura acima, o acompanhamento de 93 ações simultaneamente, referentes aos ativos operacionais em campo.

A Indústria 4.0 traz, também, a relativização da capacidade bélica pela capacidade computacional, porque ferramentas de consciência situacional, de imagem operacional comum e de sincronização de ações têm se mostrado tão poderosas quanto dispositivos explosivos, fuzis de assalto ou mesmo fuzis antimateriais 50 BMG, tanto que *drones* têm sido utilizados por Organizações Criminosas Ultraviolentas, OCUV, e Organizações Terroristas Ultrarradicais, OTUR, a fim de protagonizarem as suas ações.

Essa era está apenas começando! Muito há de ser aperfeiçoado por meio da Internet das Coisas, diante da vasta diversidade de sensores/coletores de dados e do uso de *Big Data Analytics* e de *Data Mining*, uma vez "vocacionados" para minerar dados, gerando-se *insights* em tempo real com ultravelocidade para propiciar análises preditivas. Busca-se, com essas ferramentas, o aumento da agilidade da capacidade de resposta e da eficiência na tomada de decisão, fazendo-se com que o famoso ciclo OODA seja capaz de gerar respostas com maior velocidade e resiliência.

Os conceitos de Internet das Coisas, *Machine Learning*, C*louding*, *Smart Cities*, *Data Mining*, *Data Storytelling* e *Big Data Analytics* vêm alterar significativamente a dinâmica do Gerenciamento de Incidentes, hoje no estágio C5I, e as formas de se fazer segurança pública.

3 CONCLUSÃO

A opção pelo uso do termo “incidente”, com sua forte carga preventiva, aliada à era da Quarta Revolução Industrial em ambientes VUCA, altera significativamente a forma de se gerenciar incidentes, sobretudo os policiais, dos mais simples aos mais complexos, requerendo uma estrutura de EOC capaz de prover suporte C5I com viés político-estratégico de apoio ao gerenciamento de incidentes para todos os tipos e tamanhos, em *layer* acima do local de operações e que possa ser utilizado 24/7 como um ICS/SiCOE, de maneira emergencial, até que uma estrutura de campo seja efetivada. Em nível local, é necessário que sejam adotados os conceitos e a metodologia de ICS/SiCOE, já consagrados pelo Corpo de Bombeiros, para o gerenciamento de incidentes policiais de todas as causas, tamanhos, localizações e complexidades.

A Revolução Industrial vem ajudar a entender e a resolver problemas diversos, relacionados à segurança pública, ao fornecer conceitos de *Big Data*, *Data Mining*, *Data Storytelling* e *Business Intelligence* como forma de gerar melhor consciência situacional e imagem operacional comum de incidentes de todos os tipos e tamanhos, tudo isso com a flexibilidade de aplicativos disponíveis em *smartphones*, em tempo real, agilizando a capacidade de resposta e de adaptação do estado diante de cenários VUCA.

O deslocamento do poder decisório para níveis inferiores e o foco na capacidade resposta/resiliência, além de vocacionar o Sistema de Segurança Pública para o enfrentamento de OCUV e de OTUR de forma incidental, também tem o condão de aproximar o policial decisor dos problemas mundanos que ocorrem na comunidade local. Portanto, fomenta o Patrulhamento Comunitário mais do que nunca.

O principal desafio está em como as instituições de segurança pública, notadamente as mais conservadoras, de estrutura *top down*, vão receber essa hipervigilância propiciada por toda essa tecnologia em tempo real, que não pode ser confundida como supressão de autoridade de quem decide no final da linha, mas deve ser compreendida como ferramenta subjacente de processo decisório, de apoio ao policial de rua, que decide em campo, longe dos benefícios de salas C5I, cumprindo o seu dever em meio a cenários caóticos, com elevado nível de estresse e compressão de tempo.

Certamente, esse conceito de hipervigilância focada no apoio ao policial decisor em nível local, sobretudo quanto à responsabilização em apoiá-lo, trará repercussões nas Ciências Policiais e no Direito.

REFERÊNCIAS

AGUILAR, Paulo Augusto. MACTAC - Multi-Assalut Counter-Terrorist Action Capabilities: capacidade de resposta contraterrorista frente a múltiplos ataques. **Revista A Força Policial,** São Paulo, n. 2, p. 45-57, jun. 2016. Disponível em: http://goo.gl/jNdjvo. Acesso em: 29 out. 2017.

AGUILAR, Paulo Augusto *et al.* **Atualização de procedimentos adotados na PMESP na doutrina de gerenciamento de crises, modelo estático, para o modelo dinâmico de gestão de crises**. 2017. Artigo científico (Mestrado Profissional em Ciências Policiais de Segurança e Ordem Pública) – Centro de Altos Estudos de Segurança, Polícia Militar do Estado de São Paulo, São Paulo, 2017.

CALEGARI, Luiza. As 100 cidades mais inteligentes (e conectadas) do Brasil. **Revista Exame**, São Paulo, 16 jun. 2017. Disponível em: https://exame.abril.com.br/brasil/as-100-cidades-mais-inteligentes-e-conectadas-do-brasil/. Acesso em: 22 abr. 2018.

CORPO DE BOMBEIROS DA POLÍCIA MILITAR DO ESTADO DE SÃO PAULO. Comando do Corpo de Bombeiros. **Diretriz nº CCB-004/931/14, de 16 de julho de 2014**. Sistema de Comando de Operações e Emergências (SiCOE). São Paulo: CCB, 2014.

CUNHA, Carolina. **Zygmunt Bauman**: o pensamento do sociólogo da “modernidade líquida”. [S.l.], fev. 2017. Disponível em: https://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/zygmunt-bauman-o-pensamento-do-sociologo-da-modernidade-liquida.htm?cmpid=copiaecola. Acesso em: 30 mar. 2018.

ESTADOS UNIDOS DA AMÉRICA. U.S. Department of Homeland Security. Federal Emergency Management Agency. **IS-0200.B**: ICS for Single Resource and Initial Action Incidents (ICS 200). Washington, D.C.: FEMA, 2013.

ESTADOS UNIDOS DA AMÉRICA. **National Incident Management System**. 3. ed. Washington, D.C.: FEMA, out. 2017. Disponível em: https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_20. Acesso em: 30 mar. 2018.

ESTADOS UNIDOS DA AMÉRICA. **HSPD-5**. Homeland Security Presidential Directive - Management of Domestic Incidents. Washington, D.C.: U.S. Department of Homeland Security, 2003. Disponível em: https://www.gpo.gov/fdsys/pkg/PPP-2003-book1/pdf/PPP-2003-book1-doc-pg229.pdf. Acesso em: 20 mar. 2018.

ESTADOS UNIDOS DA AMÉRICA. U.S. Department of State. Office of Antiterrorism Assistance. **Course of Critical Incident Management**. Washington, D.C.: Office of Antiterrorism Assistance, 2011.

FEW, Stephen. A better view into relationships. **Information Week**, [S.l.], 25 ago. 2004. Disponível

em: http://www.intelligententerprise.com/print_article.jhtml?articleID=31400011. Acesso em: 9 mar. 2018.

FRAZÃO, Felipe. Um drone e a digital do PCC no assalto milionário no Paraguai. **Revista Veja**, São Paulo, 28 abr. 2017. Disponível em: https://veja.abril.com.br/brasil/um-drone-e-a-digital-do-pcc-no-assalto-milionario-no-paraguai/. Acesso em: 15 abr. 2018.

FUNDAÇÃO NACIONAL DA QUALIDADE. **O que é um ambiente V.U.C.A. e o que isso tem a ver com gestão**. [S.l.], 30 nov. 2017. Disponível em: http://www.fnq.org.br/informe-se/noticias/o-que-e-um-ambiente-v-u-c-a-e-o-que-isso-tem-a-ver-com-gestao. Acesso em: 15 abr. 2018.

GUERRA, Roberto. Qual é a real diferença entre Data Storytelling e análise de dados? **CIO**, [S.l.], 20 out. 2016. Disponível em: http://cio.com.br/opiniao/2016/10/20/qual-e-a-real-diferenca-entre-data-storytelling-e-analise-de-dados/. Acesso em: 10 out. 2018.

HEAL, Charles Sid. Situational awareness and a common operational picture. **The Tactical Edge**, [S.l.], winter 2002.

KNIGHT, Judson. United States, Counter-Terrorism Policy. **Encyclopedia of Espionage, Intelligence, and Security**, [S.l.], 2004. Disponível em: www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/united-states-counter-terrorism-policy. Acesso em: 25 mar. 2018.

KOHL, Anderson. **Projetos de Simulação e de Tecnologia do EB**. Workshop de Simulação e Tecnologia Militar. [S.l.], 13 out. 2013.

MCCHRYSTAL, Stanley A. **Team of teams**: new rules of engagement for a complex world. Recife: Portfolio, 2015.

MILLS, Chuck. History of ICS. **Emergency Management Services International**, [*S.l.*], 2018. Disponível em: http://www.emsics.com/history-of-ics. Acesso em: 14 abr. 2018.

MONTEIRO, Roberto das Chagas. **Manual de gerenciamento de crises**. Brasília: Departamento de Polícia Federal, 1994.

POLÍCIA MILITAR DO ESTADO DE SÃO PAULO. **Diretriz nº PM3-008/02/06, de 11 de agosto de 2006**. Normas para o Sistema Operacional de Policiamento PM (NORSOP). São Paulo: PMESP, 2006.

SCACHETTI JÚNIOR, Paulo Luiz. **Sistema de Comando e Controle**: análise conceitual e perspectiva de utilização conjunta pela Polícia Militar, Corpo de Bombeiros e Defesa Civil do estado de São Paulo. 2014.Tese (Doutorado em Ciências Policiais de Segurança e Ordem Pública) – Centro de Altos Estudos de Segurança, Polícia Militar do Estado de São Paulo, São Paulo, 2014.

SOUZA, Wanderley Mascarenhas de. **Gerenciamento de crises:** negociação e atuação de grupos especiais de polícia na solução de eventos críticos. 1995. Monografia (Curso de Aperfeiçoamento de Oficiais) – Centro de Aperfeiçoamento e Estudos Superiores, Polícia Militar do Estado de São Paulo, São Paulo, 1995.

Submetido em 07/11/2019 e aceito para publicação em 01/01/202