# A INTEGRAÇÃO DA GEOINT E CYBINT EM CONFLITOS RECENTES

**Joffre Ferreira Abdalla**

Capitão de Artilharia do Exército Brasileiro, Bacharel em Ciências Militares – Academia Militar das Agulhas Negras (AMAN) e pós-graduado em Ciências Militares – Escola de Aperfeiçoamento de Oficiais (ESAO). Atualmente serve no 6º Batalhão de Inteligência Militar (6º BIM) e possui o Curso de Geointeligência.

**TC José Alves Júnior**

Orientador

## 1. INTRODUÇÃO

A evolução exponencial dos meios de tecnologia da informação e comunicação (MTIC) aumentou a circulação de informações através da rede de computadores, a internet. Dessa forma, nas últimas décadas, tal rede se tornou uma das principais fontes de dados e informações para a sociedade (SILVA e SCHERER, 2019). Nesse contexto, temos o espaço cibernético, um ambiente digital composto por redes de computadores, onde os dados e as informações circulam e são armazenadas (BRASIL, 2015a).

Esse desenvolvimento tecnológico marcou a sociedade, pois a comunicação global se tornou instantânea e muitas atividades cotidianas saíram do ambiente físico e foram otimizadas no ambiente virtual de dados e informações.

Segundo o Manual de Campanha Operações, do Exército Brasileiro, nos conflitos atuais têm predominado combates em terrenos humanizados, com a inserção de atores não estatais que agem em espaços que vão além do campo de batalha. A dimensão informacional composta por sistemas utilizados para obter, produzir, difundir e atuar sobre a informação possui destacada importância, tendo em vista a elevada capacidade da sociedade de transmitir, acessar e compartilhar a informação (BRASIL, 2017a).

Ainda conforme o supracitado manual, alguns aspectos do ambiente operacional são relevantes na conjuntura atual, tais como: a expansão de novas tecnologias em materiais de emprego militar e o emprego dos meios cibernéticos e informacionais por indivíduos ou grupos não estatais, como ferramentas de guerra, capazes de afetar diretamente o poder de combate dos beligerantes estatais (BRASIL, 2017).

Acompanhando essa expansão tecnológica no ambiente operacional, o Exército Brasileiro passou a tratar em seus manuais sobre as disciplinas de inteligência, dentre elas a GEOINT (*Geospatial Intelligence* ou Inteligência Geográfica, ou ainda, Inteligência Geoespacial) e a CYBINT (*Cyber Intelligence* ou Inteligência Cibernética), que tiveram suas capacidades ampliadas pelas evoluções dos MTIC e hoje são capazes de otimizar o conhecimento produzido pela Função de Combate Inteligência em proveito do processo decisório (BRASIL, 2015b).

No panorama dos conflitos armados dos últimos dez anos (2012-2022), tem sido constatado que agentes não estatais, tem realizado atividade de inteligência, através da integração das disciplinas GEOINT e CYBINT, para obtenção, análise e difusão de informações na internet, que poderiam interferir nos planos de batalha das forças beligerantes.

## 2. A GEOINTELIGÊNCIA NO ESPAÇO CIBERNÉTICO

Conforme o manual MD35-G-01, do Exército Brasileiro (BRASIL, 2015a), a Geointeligência se caracteriza pela integração, interpretação e análise de dados georreferenciados de interesse militar presentes no espaço de batalha, com a intenção de produzir conhecimento que apoiem o processo decisório.

Clark (2020) complementa que a inteligência geoespacial pode ser tanto um processo que consiste na exploração e na análise, quanto um produto de representação visual, em que ambas as definições utilizam fontes específicas tais como imagens, inteligência de imagens e informações geográficas.

A evolução da GEOINT está estritamente relacionada ao desenvolvimento computacional, o qual proporcionou a criação e a evolução do Sistema de Informações Geográficas (SIG ou GIS). A idéia principal do SIG está relacionada ao uso de computadores para fornecer mapas digitais com maiores detalhamentos e informações, que estariam vinculadas de forma organizada a bancos de dados digitais (CLARK, 2020).

Dessa maneira, inserimos o espaço cibernético como principal ambiente para o desenvolvimento das operações de inteligência geoespacial, tendo em vista que a coleta, circulação e a produção de seus dados e conhecimentos de inteligência estão predominantemente presentes no ambiente informacional digital, através de redes de compartilhamento, programas computacionais para processamento digital de imagens ou para confecção de produtos gráficos, tais como os mapas temáticos.

Além dos bancos de dados federais, na internet são encontrados outros repositórios alternativos para pesquisa de dados geoespaciais. Principalmente no que tange à capacidade de atualização temporal, as Interfaces de Programação de Aplicação (*Application Programming Interface* – API) de sites de empresas que utilizam o metadados como o *Google* e o *Strava* são opções para atualização e obtenção de dados geoespaciais de atividades mais específicas como localização de eventos, até mesmo nos cenários de guerra atuais da Guerra da Ucrânia e Rússia.

Segundo a empresa AWS (2022), os APIs **são mecanismos que possibilitam a comunicação entre dois** *softwares* (cliente-servidor) para transmissão de dados atualizados automaticamente. Como exemplo, mencionamos um aplicativo de *smartphone* de condições climáticas (cliente) que atualiza suas informações através da comunicação com o API de um instituto meteorológico (servidor) que lhe tenha autorizado a conexão para transmissão de seus dados.

Ainda no contexto de fontes de dados para a GEOINT, temos as redes sociais como fontes importantes para a IMINT (inteligência de imagens), que como mencionado anteriormente é um vetor componente da inteligência Geográfica. Através da realização de uma OSINT (inteligência de fontes abertas) nas redes sociais como o *Instagram* e o *Facebook*, podem ser obtidas imagens, vídeos e marcação de localizações em publicações que possibilitam a identificação de alvos de interesse da IMINT/GEOINT.

Atualmente, até mesmo os aplicativos de atletas como *Strava*, *Garmin* e *Polar* podem ser utilizadas para a obtenção de metadados georreferenciados ou da localização de alvos de interesse através de

**Figura 1** - Integração de GEOINT e CYBINT.

Fonte: Bing Image Creator (2023).

rotas e percursos compartilhados pelos usuários ou pelo mapa de calor das regiões gerados pelo aplicativo em seu site na internet. Tal assunto será abordado mais amplamente no próximo capítulo.

## 3. A INTELIGÊNCIA CIBERNÉTICA EM PROVEITO DA GEOINTELIGÊNCIA

A CYBINT se caracteriza por ações de exploração no espaço cibernético com o intuito de obter dados de interesse (BRASIL, 2014). Tal prática é comum entre as forças armadas de diversos países, tais como Estados Unidos da América (EUA), Rússia e China (CLARKE, 2015).

Pela relevância de conteúdo disponível como dados ou informações, nos últimos anos, os agentes não-estatais aumentaram sua presença no espaço cibernético com intuito de ampliar seu quadro de referência na análise e produção de conhecimentos de inteligência. Na maioria dos casos, observa-se que tais agentes não violaram banco de dados para adquirir o dado digital, apenas se utilizaram da internet para explorar e obter dados disponibilizados no espaço cibernético.

Durante um conflito bélico iniciado em 2014, em que as regiões ucranianas de Donetsk e Criméia foram disputadas entre a Rússia e a Ucrânia, ocorreu a integração entre as disciplinas CYBINT e GEOINT. Conforme o colunista Will Wisser, do site *My Spybot* (2017), um aplicativo de celular desenvolvido por militares ucranianos para auxiliar nos cálculos dos elementos de tiro de artilharia foi contaminado por um código malicioso desenvolvido por hacker russos, um grupo denominado *Fancy Bear*.

O referido código batizado como X-Agent tinha como alvo o aplicativo Popr-D30 (original em ucraniano Попр-Д30), desenvolvido por um oficial da 55ª Brigada de Artilharia das Forças Armadas Ucranianas para auxiliar nos cálculos de elementos de tiro do obuseiro D-30, de 122 mm. O aplicativo conseguia reduzir o tempo de tiro, que antes era superior a um minuto, para um tempo de quinze segundos. Tal façanha fez com que o aplicativo fosse distribuído abertamente entre militares ucranianos através de fóruns na internet. Estima-se que aproximadamente nove mil militares tenham baixado a aplicação em seus celulares entre 2014-2016.

Entretanto, durante esse período, o grupo *hacker* conseguiu, de modo furtivo, obter uma cópia do aplicativo e reconstruí-lo inserindo o código malicioso X-Agent. Em seguida a versão contaminada foi disponibilizada nos mesmos fóruns militares ucranianos (WISSER, 2017). Dessa forma, quando o aplicativo contaminado estava ativado nos celulares providos de sistema operacional *android*, durante os combates, o grupo *hacker* obtinha os dados de geolocalização dos artilheiros ucranianos e, consequentemente, da posição de suas peças de artilharia (MEYERS, 2016).

Estima-se que essa ação cibernética para obtenção de dados, integrada com a GEOINT, tenha possibilitado que as tropas russas infligissem aos artilheiros ucranianos uma perda de 80% dos obuseiros D-30 empregados nos combates entre 2014 e 2016 (WISSER, 2017).

Outra atividade integradora entre CYBINT e GEOINT ocorreu através do aplicativo *fitness Strava*, que revelou a localização de bases militares, enquanto os usuários publicavam a rota de seus exercícios na comunidade do aplicativo (WALLACE, 2022).

O aplicativo rastreia, através do *Global Positioning System* (GPS) de *smartphones* ou *smartwatchs*, as rotas de corridas e ciclismo realizadas pelos seus usuários. Após o compartilhamento no aplicativo, o *Strava* gera e disponibiliza mapas de calor (*heat maps*) em sua comunidade online. Tais mapas mostram abertamente os caminhos mais registrados por seus usuários

enquanto praticam atividade física com o rastreamento do aplicativo ativado.

Os mapas de calor do *Strava* tiveram repercussão internacional em 2017, quando o estudante australiano Nathan Ruser identificou bases militares estadunidenses ativas em países como Síria e Afeganistão através desses mapas e divulgou a informação na rede social *Twitter* (BBC, 2018).

Embora a localização das bases militares seja geralmente conhecida e as imagens de satélite possam mostrar o contorno das construções, o mapa de calor pode revelar quais delas são mais utilizadas, ou as rotas percorridas pelos soldados durante as patrulhas através da intensidade do "calor" da rota no mapa. Logo após a repercussão supracitada, outras bases militares foram expostas, tais como uma instalação militar italiana em Djibuti e outras francesas no Níger e no Mali.

No conflito mais recente entre Ucrânia e Rússia iniciado em 2022, os mapas de código aberto têm desempenhado um papel importante desde o início da invasão russa. Através da aplicação *Google Earth*, um professor da Califórnia, detectou uma concentração suspeita de veículos militares russos na estrada de Belgorod, na Rússia, em direção a Kharkiv, na Ucrânia. Em seguida, um de seus alunos de pós-graduação monitorou um acúmulo de veículos e armas militares em imagens de satélite através de linhas de códigos inseridos no *Google Earth Engine*. Juntando as duas informações, eles previram a invasão da Ucrânia antes de Vladimir Putin anunciar o início das operações militares (SOOIN, 2022).

Ainda segundo SOOIN (2022), na mesma linha de raciocínio, a comunidade ucraniana do *Open Street Map* pediu aos voluntários que deixassem de editar o mapa do território ucraniano até que a guerra terminasse. Atualizar a localização das principais instalações de infraestrutura pode ser útil para os ucranianos, mas essas informações também podem ser facilmente acessadas pelos militares russos.

Nesse mesmo conflito, em alguns casos as disciplinas e fontes CYBINT e HUMINT se integram naturalmente. Conforme Sophia Ankel publicou no site *Business Insider* (2022), o grupo ucraniano de *hackers Hackyourmom* (agentes não-estatais) reuniu aproximadamente trinta voluntários para descobrir a localização das tropas russas.

Para atingir seu objetivo, o grupo aplicou uma técnica conhecida como *catfishing:* utilizou aplicativos de comunicação como o *Telegram* para se passarem por mulheres através de perfis falsos e assim obterem a localização de bases russas. As vítimas da engenharia social aplicada pelos *hackers* foram os soldados russos que estavam na linha de frente do combate. Os agentes não-estatais conseguiram induzir os militares para que enviassem suas imagens na linha de frente, sem saber que elas poderiam revelar sua localização, pois os *smartphones* modernos incorporam coordenadas de GPS em todas as fotos tiradas (ANDERSON, 2022), ou através da inteligência de imagens (IMINT).

O chefe do grupo, Nikita Knysh, revelou que dentre as imagens recebidas, os *hackers* conseguiram identificar uma base militar russa na fábrica Avtokoliorlyt, próximo de Melitopol, cidade ucraniana ocupada pelos russos. Essa informação foi transmitida às forças militares ucranianas, que no final do mês de agosto de 2022, atacaram a referida posição estratégicas russa.

## 4. CONCLUSÃO

Durante a pesquisa deste artigo, foi possível identificar que os conflitos bélicos atuais entre as nações receberam novos atores, os agentes não-governamentais, capazes de interagir no ambiente operacional até o ponto de produzir efeitos nas decisões militares em níveis táticos, operacionais ou estratégicos.

Foi constatada a imersão da GEOINT no espaço cibernético, devido à grande tramitação e disponibilidade de dados geoespaciais no referido ambiente. Geralmente esses dados podem ser obtidos de modo lícito através de pesquisa a bancos de dados geográficos mantidos pelos governos ou por comunidades de desenvolvedores de aplicações do Sistema de Integração Geográfica (SIG).

Tendo em vista que a disciplina CYBINT é concebida a partir de dados, protegidos ou não, obtidos no ambiente cibernético, foi observado que, em conflitos armados dos últimos dez anos (2012-2022), os agentes não estatais têm integrado as disciplinas GEOINT e a CYBINT para obtenção, análise e difusão de informações na internet que podem interferir nos planos de batalha das forças beligerantes.

Destarte, este artigo buscou expor a integração entre a GEOINT e a CYBINT nas atividades de inteligência realizadas por agentes não governamentais para constatar que tal integração tem aplicação viável na doutrina militar. O produto de tal integração é um conhecimento mais completo, com maior capacidade de visualização gráfica e precisão na localização geoespacial inserido no ambiente operacional.

Através dessa exposição, também foi possível constatar que em alguns casos, o produto de tal integração por agentes não estatais tem sido remetido às forças armadas para que elas tirassem proveito do conhecimento produzido. Como por exemplo, os alvos militares levantados geograficamente por ambos países beligerantes nos conflitos entre Rússia e Ucrânia.

Dessa forma, estima-se que a integração das disciplinas de GEOINT e CYBINT por parte da inteligência militar da Força Terrestre poderá produzir conhecimentos que diminuam incertezas do processo decisório no ambiente operacional dos conflitos de 4ª geração.

## REFERÊNCIAS


1. ANDERSON, Katie. **Catfishing the enemy**: how ukrainian hackers are discovering russian locations. How Ukrainian Hackers are Discovering Russian Locations. 2022. Disponível em: https://ethicalgeo.org/elementor-4092/. Acesso em: 22 out. 2022
2. ANKEL, Sophia. **Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says – Days later, the base was blown up**. 2022. Disponível em: https://www.businessinsider.com/ukraine-hackers-create-fake-profiles-russia-troops-share-location-ft-2022-9. Acesso em: 22 out. 2022.
3. BBC. **Fitness app Strava lights up staff at military bases**. 2018. Disponível em: https://www.bbc.com/news/technology-42853072. Acesso em: 04 set. 2022.
4. BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Glossário das Forças Armadas – MD-35-G-01.** 5. ed. Brasília, DF, 2015a.
5. BRASIL. Ministério da Defesa. Estado-Maior do Exército. **Manual de Campanha Operações – EB70-MC-10.223.** Brasília, DF, 2017a.
6. BRASIL. Ministério da Defesa. Estado-Maior do Exército. **Guerra Cibernética – EB70-MC-10.232.** Brasília, DF, 2017b.
7. BRASIL. Ministério da Defesa. Exército Brasileiro. **Manual de Fundamentos Inteligência Militar Terrestre – EB-20-MF-10.107**. Brasília, DF, 2. Edição/2015b.
8. CLARK, Robert M. **Geospatial Intelligence**: origins and evolution. Washington, DC: Georgetown University Press, 2020. p. 496.
9. CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. ed. Kindle. Rio de Janeiro: Brasport, 2015.

10. HSU, Jeremy. **The Strava eat map and the end of secrets.** 2018. Disponível em: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/. Acesso em: 04 set. 2022.
11. MEYERS, Adam. **Danger close**: fancy bear tracking of ukrainian field artillery units. 2016. Disponível em: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/. Acesso em: 22 out. 2022.
12. SILVA, Lauro D.S.; SCHERER M. V. **Emprego de coleta especializada em proveito da Atividade de Inteligência**. Brasília, 2019.
13. SOOIN, Choi. **Open street map**: disputed territories. disputed territories. 2022. Disponível em: https://ethicalgeo.org/openstreetmap-disputed-territories/. Acesso em: 22 out. 2022.
14. STRAVA. **Heatmap**. 2022. Disponível em: https://www.strava.com/heatmap. Acesso em: 22 out. 2022.
15. WALLACE, Michael. **Geospatial technologies and war**. 2022. Disponível em: https://ethicalgeo.org/geospatial-technologies-and-war. Acesso em: 17 ago. 2022.
16. WISSER, Will. **Fancy Bear tracking Ukrainian artillery units**. 2017. Disponível em: https://myspybot.com/fancy-bear-tracking-ukrainian-artillery-units/. Acesso em: 22 out. 2022.