ipea Instituto de Pesquisa Econômica Aplicada

Título do capítulo	CAPÍTULO 12 **DESMISTIFICANDO A SEGURANÇA NACIONAL PARA MECANISMOS DE TRIAGEM DE INVESTIMENTO ESTRANGEIRO DIRETO: POR QUE A CRITICIDADE IMPORTA?**
Autor(es)	Manu Misra
DOI	DOI: https://dx.doi.org/10.38116/9786501305431cap12

Título do livro	**Instrumentos de avaliação de investimentos externos no mundo e seus debates no Brasil**
Organizadores	Michelle R. Sanchez-Badin Renato Baumann
Volume	1
Série	-
Cidade	Rio de Janeiro
Editora	Instituto de Pesquisa Econômica Aplicada (Ipea)
Ano	2025
Edição	1a
ISBN	9786501305431
DOI	DOI: https://dx.doi.org/10.38116/9786501305431

© Instituto de Pesquisa Econômica Aplicada – ipea 2025

As publicações do Ipea estão disponíveis para *download* gratuito nos formatos PDF (todas) e EPUB (livros e periódicos). Acesse: https://repositorio.ipea.gov.br/

As opiniões emitidas nesta publicação são de exclusiva e inteira responsabilidade dos autores, não exprimindo, necessariamente, o ponto de vista do Instituto de Pesquisa Econômica Aplicada ou do Ministério do Planejamento e Orçamento.

É permitida a reprodução deste texto e dos dados nele contidos, desde que citada a fonte. Reproduções para fins comerciais são proibidas.

CAPÍTULO 12

DESMISTIFICANDO A SEGURANÇA NACIONAL PARA MECANISMOS DE TRIAGEM DE INVESTIMENTO ESTRANGEIRO DIRETO: POR QUE A CRITICIDADE IMPORTA?

Manu Misra[1]

1 INTRODUÇÃO

Apesar de seu uso cada vez mais comum nas discussões contemporâneas sobre investimento estrangeiro, incluindo tanto a literatura acadêmica quanto o discurso popular, o termo "segurança nacional" continua opaco, mal definido e, portanto, aberto a possíveis abusos. De fato, historicamente, a percepção predominante é que as afirmações de segurança nacional na formulação de políticas econômicas, sejam elas feitas por maus formuladores de políticas ou analistas, provavelmente são falsas, sendo o protecionismo ou o nacionalismo econômico os verdadeiros motivos subjacentes. Essa má reputação e a presunção de má-fé não foram sem motivo. Registra-se que, sob o manto da segurança nacional, tanto os Estados democráticos quanto os autocráticos abusaram de seus poderes discricionários executivos, seja internamente, em relação a atores internos, para manter seu controle sobre o poder, suprimindo os direitos fundamentais dos cidadãos e restringindo a liberdade de imprensa, seja internacionalmente, para justificar invasões estrangeiras, intervenções armadas e espionagem ilegal.

No entanto, apesar da bagagem histórica que o termo segurança nacional carrega, será que as afirmações contemporâneas a seu respeito no contexto do investimento estrangeiro direto (IED) devem continuar a ser recebidas com o mesmo grau de suspeita? Ou, em vez disso, as circunstâncias atuais são diferentes e existem, de fato, algumas formas novas e legítimas de ameaças à segurança nacional que podem fornecer justificativas válidas para que o Estado intervenha no mercado de IED? Mais importante ainda, existe, portanto, uma noção de segurança nacional no contexto do investimento estrangeiro que possa ser universalmente aplicável para apoiar afirmações de boa-fé e empiricamente

1. Pesquisador no Centro de Tecnologia e Sociedade (CTS) da Escola de Direito da Fundação Getulio Vargas do Rio de Janeiro (FGV Rio de Janeiro); bolsista de pós-doutorado da Escola de Direito da FGV São Paulo; bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes); mestre em direito e economia pela Universidade de Hamburgo; e PhD em estudos jurídicos (direito internacional e economia) pela Universidade Bocconi, em Milão. *E-mail*: manu.misra@bocconialumni.it.

fundamentadas que possam ser distinguidas das tentativas de protecionismo velado ou nacionalismo econômico?

Este texto procura abordar essa questão, que continua a desafiar o pensamento acadêmico e profissional, expondo a noção de "criticidade", conforme ela evoluiu no campo dos estudos de segurança e atualmente está emergindo nas regras que regem os mecanismos de triagem de investimento estrangeiro (*investment screening mechanisms* – ISMs), globalmente. Em particular, discutem-se a infraestrutura crítica (*critical infrastructure* – CI) e os dados críticos (*critical data* – CD) como duas categorias de ativos que se inter-relacionam com a dimensão de investimento estrangeiro da segurança nacional ("segurança do investimento estrangeiro") e são amplamente observáveis nos ISMs de nova geração. Distinguem-se essas duas categorias das tecnologias críticas (*critical technology* – CT), ao mesmo tempo que se questiona a adequação dessa terceira categoria a uma questão de segurança nacional, conforme conceituada aqui, além de sua aplicação militar e de CI.

Em seguida, argumenta-se que, no contexto da segurança do investimento estrangeiro, o termo "crítico", conforme derivado dos estudos de segurança, está relacionado a um conceito específico que é distinto de outros, como "sensível" e "estratégico", e usar esses termos de forma intercambiável, como geralmente acontece, seria errôneo e contrário ao objetivo de aumentar a clareza.

Por fim, conclui-se que, para compreender plenamente as novas fronteiras da segurança econômica, é preciso atenuar as suspeitas anteriormente mantidas e permitir que as noções tradicionais de que se constituem os interesses de segurança de um Estado evoluam, avaliando a criticidade inerente de certos tipos de ativos econômicos e as implicações de segurança de boa-fé resultantes dessa característica qualitativa. Para fundamentar os argumentos e ajudar a esclarecer as considerações de segurança nacional no contexto da política de investimento estrangeiro, este capítulo adota uma abordagem interdisciplinar, combinando discussões conceituais de estudos de segurança com análises de direito econômico comparado.

2 CRITICIDADE COMO NOÇÃO GERAL

Um conceito há muito debatido no campo dos estudos de segurança, a noção de criticidade surgiu amplamente nos últimos anos nas regras do ISM, com vários Estados buscando explicitamente delinear e exercer controle sobre a propriedade e o acesso a ativos que eles consideram críticos.

Em 2016, a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) já havia observado que "a referência a setores estrategicamente importantes e à infraestrutura essencial é hoje muito mais frequente do que há seis anos, quando a segurança nacional era definida em um sentido

muito mais restrito" (Wehrlé e Pohl, 2016, p. 22, tradução nossa). Da mesma forma, a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (United Nations Conference on Trade and Development – UNCTAD), em seu relatório sobre investimentos mundiais do mesmo ano, observou que as considerações de segurança nacional estavam ganhando destaque nas políticas de investimento e que "os países usam diferentes conceitos de segurança nacional, desde uma definição relativamente restrita até interpretações mais amplas que estendem os procedimentos de revisão de investimentos a infraestruturas críticas, setores estratégicos e/ou considerações de interesse nacional" (UNCTAD, 2016, p. 94, tradução nossa). Além disso, "novas restrições ou regulamentações de investimento para investidores estrangeiros foram baseadas principalmente em preocupações com a propriedade estrangeira de infraestrutura crítica" (UNCTAD, 2018, p. 80, tradução nossa). Ainda segundo UNCTAD (2018, p. 85, tradução nossa), "em 2017, vários governos de países anfitriões levantaram objeções a várias tentativas de aquisição estrangeira, em particular quando elas envolviam a venda de ativos domésticos críticos ou estratégicos a investidores estrangeiros".

Desde então, o termo crítico, originado e com maior evolução no campo da proteção de CI e de estudos de segurança mais amplos, tem sido cada vez mais visível nas regras de ISM, um fenômeno que não foi de forma alguma uma coincidência, visto que tanto a proteção de CI quanto os ISMs têm um objetivo subjacente comum de garantir a segurança nacional, com o último atingindo seu auge muito depois de o primeiro ter amadurecido como um campo. Com a maior proliferação de ISMs, o uso do termo CI também se expandiu, e o conceito recebeu maior atenção no campo da política de investimento estrangeiro (Misra, 2023).

Exemplos recentes e proeminentes disso incluem a designação pela Austrália de todas as "entidades responsáveis" e "detentores de participação direta" de ativos de CI como "empresas de segurança nacional" nas quais um investidor estrangeiro não pode obter participação direta sem aprovação do Estado, independentemente da nacionalidade ou do valor da empresa (Firb, 2021); e a expansão pela Alemanha da categoria de empresas designadas como operadoras de CI para incluir também prestadores (inclusive terceiros) de serviços (como tecnologia da informação – TI, finanças, seguros e saúde) aos operadores de CI, sujeitando, assim, quaisquer transações de investimento estrangeiro que eles possam tentar concluir a obrigações de notificação nos termos do ISM alemão[2] ou das medidas

2. Além de estarem sujeitas a maiores medidas de mitigação de riscos relacionados à segurança cibernética. Consulte a segunda alteração da Portaria sobre a Designação de Infraestruturas Críticas nos termos da Lei Bundesamt für Sicherheit in der Informationstechnik (BSI), que entrou em vigor em 7 de maio de 2021. Disponível em: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Rechtsgrundlagen/rechtsgrundlagen_node.html.

de Revisão da Segurança Nacional de 2020 da China, que ampliaram o escopo do ISM chinês "de atividades relacionadas à defesa nacional para CI, tecnologia avançada e conteúdo digital, como dados pessoais" (Kong e Li, 2021, p. 5).

Nos últimos anos, a atenção acadêmica do campo da lei de investimento internacional também se voltou para a existência de "uma abertura da definição do termo segurança nacional para incluir também considerações além da segurança nacional no sentido estrito" (Dimitropoulos, 2020, p. 36). Entretanto, embora as observações acerca do termo crítico no direito econômico e na formulação de políticas tenham sido feitas com frequência, não foi dada muita atenção ao significado ou à origem do termo em si e à distinção qualitativa que ele carrega.

Se um ativo, físico ou virtual, pode ser considerado crítico é, em grande parte, uma questão objetiva que considera o nível de importância desse ativo para o funcionamento de uma economia ou sociedade. Um ponto importante que vale a pena enfatizar é que a criticidade, em seu sentido puro derivado de estudos de segurança, não está relacionada à concorrência, e que o fato de um ativo (físico, virtual ou humano) ser importante para a competitividade de um Estado na economia global não o torna, por si só, crítico se a perda ou a interrupção desse ativo não levar a graves consequências econômicas ou sociais em escala nacional. Somente quando a perda ou a interrupção de tal ativo puder levar a consequências negativas que afetem o funcionamento de uma economia ou sociedade é que ele poderá ser considerado crítico e afetar a segurança nacional.[3]

Por exemplo, se considerarmos o setor de produtos de luxo ou o setor de produtos de consumo da linha branca, eles consistem em ativos que, se forem interrompidos, não terão consequências tão graves e generalizadas que afetem negativamente o funcionamento de uma economia ou sociedade nacional. No entanto, o setor de energia ou de telecomunicações é composto por esses ativos. Afinal, sem eletricidade ou serviços de internet, a maioria das empresas e residências deixaria de funcionar, enquanto o mesmo não pode ser dito sobre relógios de pulso ou eletrodomésticos de alta qualidade.[4]

A filtragem da criticidade, conforme conceituada aqui, de um ativo econômico subjacente a uma transação de IED proposta nos permite, portanto, separar *objetivamente* as propostas que podem representar uma possível ameaça à segurança nacional daquelas que não representariam, uma vez que a criticidade, em última análise, diz respeito a atividades que facilitam o fornecimento das necessidades

3. Essa perda no funcionamento da sociedade não é apenas um ataque em si (e, portanto, uma ameaça direta à segurança), mas também enfraquece o mecanismo do Estado para lidar com ataques militares tradicionais.

4. Essa característica qualitativa distinta da criticidade também é evidente na definição do termo no dicionário Oxford, que diz "ter uma importância decisiva ou crucial no sucesso, fracasso ou existência de algo".

básicas exigidas para a sobrevivência diária de todos os seres humanos (como alimentos, energia, abastecimento de água, assistência médica etc.) e sua segurança física.

Como a interrupção ou a manipulação de ativos não críticos não levaria a consequências negativas para o atendimento das necessidades humanas básicas, mesmo que um investimento estrangeiro proposto por um agente mal-intencionado seja permitido, não haveria canais de ameaça ou vulnerabilidades a serem explorados por ele. No entanto, seria razoável rejeitar, ou pelo menos ser cético, as afirmações de riscos à segurança nacional feitas nesses setores.

A noção de criticidade, contudo, assume uma camada adicional de complexidade quando um elemento de relatividade é introduzido, em que nem todos os ativos específicos dentro de uma categoria amplamente crítica são necessariamente considerados igualmente críticos e, portanto, garantem o mesmo nível de escrutínio para transações de IED relacionadas. Isso é visível, por exemplo, na Estratégia Nacional Alemã para a Proteção de Infraestruturas Críticas de 2009, que define a criticidade como "uma medida relativa das consequências de uma perturbação ou falha de função relativa ao fornecimento de bens e serviços à sociedade".[5] Isso também é visível, por exemplo, na "escala de criticidade" do Reino Unido, que atribui categorias a diferentes graus de gravidade em termos do impacto que a interrupção de um ativo específico teria sobre o funcionamento da sociedade, incluindo o impacto econômico, na vida humana e nos serviços essenciais (United Kingdom, 2010).

Esse aspecto da relatividade como indicador ou medida da criticidade de um ativo específico, e não apenas de um tipo de ativo, diz respeito ao grau de consequência que a interrupção ou manipulação desse ativo específico teria sobre a rede mais ampla de ativos a que pertence e, em última análise, sobre o funcionamento da sociedade ou da economia em escala nacional. Esse é um fator extremamente importante, uma vez que permite que as autoridades de ISM façam a diferenciação entre vários ativos dentro de uma categoria específica e, consequentemente, tomem decisões de ISM mais matizadas e apropriadas, em termos de quais transações devem ser consideradas muito arriscadas para serem permitidas, quais podem ser permitidas com condições de mitigação de risco e quais não representam risco suficiente para exigir qualquer ação em relação a elas.

Por exemplo, embora os portos marítimos e as rodovias internacionais pudessem, em geral, ser razoavelmente considerados ativos críticos, determinados segmentos de rodovias e portos marítimos nacionais seriam mais críticos que outros se fornecessem conexões exclusivas entre as principais cidades ou fossem essenciais para o funcionamento de uma cadeia de suprimentos vital que apoiasse

5. Disponível em: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1.

o setor de serviços de saúde ou o Exército. Em contrapartida, segmentos alternativos dentro da mesma rede, que na prática não atendiam a nenhuma dessas finalidades e serviam não exclusivamente a duas pequenas cidades com conexões alternativas, seriam considerados menos críticos, visto que uma manipulação ou interrupção nesses ativos não teria um impacto negativo importante nos serviços do setor de transporte mais amplo e no funcionamento da economia nacional.

Uma boa tomada de decisão sobre o ISM refletiria essa distinção, e as afirmações de segurança nacional, por exemplo, no setor de transportes precisariam estabelecer, entre outras coisas, o impacto relativo do ativo específico subjacente a uma transação proposta, e não apenas apontar a criticidade da infraestrutura de rodovias ou portos marítimos em geral. Estimar o grau adequado de criticidade do ativo econômico subjacente, em relação à rede e ao ecossistema ao qual ele pertence, é, portanto, um exercício crucial na avaliação dos riscos à segurança nacional de uma determinada transação de IED proposta. Enquanto a superestimação da criticidade pode levar ao condicionamento ou bloqueio desnecessário das transações de IED, uma subestimação levaria a que os riscos de segurança não fossem corretamente identificados e fossem indevidamente permitidos.

3 INFRAESTRUTURA CRÍTICA

Conforme exemplificado, uma categoria importante de ativos críticos é a CI. Esses ativos deixaram de ser uma preocupação primordial do setor privado, vista sob a ótica do desenvolvimento e da eficiência, e passaram a ser uma preocupação do Estado, vista sob a ótica da segurança nacional e da resiliência. Essa mudança se deve, em parte, a um aumento na complexidade dos mecanismos de ameaça e a uma maior integração de TI às estruturas físicas. Em termos de definição específica de CI, embora existam algumas diferenças entre as várias jurisdições quanto à forma de os Estados abordarem a questão,[6] as definições tendem a seguir linhas como a própria noção de criticidade. Nos Estados Unidos, por exemplo, a CI é considerada uma infraestrutura tão vital que sua destruição "teria um impacto debilitante na segurança nacional".[7] Mais especificamente, os ativos críticos são definidos como "sistemas e ativos, físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou destruição de tais sistemas ou ativos teria um impacto debilitante na segurança nacional" (tradução nossa).[8]

6. Diz-se que a primeira definição formal de CI por um governo federal teve origem nos Estados Unidos durante a administração Clinton, que estabeleceu a Comissão Nacional de Proteção de Infraestrutura Crítica dos Estados Unidos em 1996. Para mais informações, conferir a Ordem Executiva nº 13.010, Critical Infrastructure Protection, disponível em: irp.fas.org/offdocs/eo13010.htm. Conferir também White Paper: Clinton Administration's Policy on Critical Infrastructure Protection, disponível em: clintonwhitehouse4.archives.gov/WH/EOP/NSC/html/documents/NSCDoc3.html; e Gallais e Filiol (2017).

7. Ver seções 2(a), 5 e 6 do *Foreign Investment and National Security Act of 2007*, dos Estados Unidos. Disponível em: https://www.congress.gov/110/plaws/publ49/PLAW-110publ49.pdf.

8. Disponível em: https://www.law.cornell.edu/uscode/text/42/5195c#e.

No entanto, em termos gerais, como conceito, seguindo a noção geral de criticidade descrita anteriormente, a CI tende a abranger ativos considerados vitais para o funcionamento de uma economia (ou de uma sociedade em geral), cuja perda ou interrupção levaria a graves consequências econômicas ou sociais, em escala nacional. Instalações de energia, serviços públicos, transporte, portos internacionais e redes de telecomunicações são, portanto, alguns dos principais exemplos de ativos que são frequentemente designados como CI.[9] O fato de estarem intrinsecamente ligados às necessidades humanas básicas faz com que a criticidade de tais ativos seja uma característica objetivamente identificável e inevitável.[10]

Embora o aumento das referências e da conscientização sobre o conceito de CI nos ISMs como forma de segurança econômica seja um fenômeno relativamente recente, o debate em torno dela existe há várias décadas: primeiro com ênfase principalmente na segurança física, e à medida que houve maior progresso tecnológico, evoluiu em grande parte para um debate altamente técnico com foco maior na segurança cibernética.

A esfera anterior que envolve a segurança física da CI tem origem na doutrina militar e, embora também envolva a proteção contra desastres naturais, como enchentes e terremotos, uma grande preocupação que também impulsionou seu desenvolvimento histórico foi a proteção da infraestrutura essencial contra ataques físicos adversários.[11] No entanto, atacar a CI do adversário também tem sido considerado uma estratégia militar eficiente e procurada, em parte devido à interdependência entre as várias formas de CI. Por exemplo, quase todas essas formas precisam de energia (e, atualmente, de conectividade com a internet) para funcionar e, portanto, atacar a primeira pode debilitar as outras também, compondo assim o efeito pretendido além do alvo imediato.

Com o progresso tecnológico e a maior conectividade surgindo e aumentando exponencialmente da década de 1980 até a década de 2000, incluindo o uso privado e civil, as redes de TI se tornaram cada vez mais integradas à CI, o que, por sua vez, criou canais novos, mais sofisticados e discretos de ataques

9. Além de sua criticidade, outra característica marcante da CI que vale a pena reconhecer é seu elemento "nacional". Ou seja, os riscos associados a ela, independentemente de sua definição, são, em última análise, vivenciados coletivamente por todos dentro de um limite territorial, em nível nacional. Essa natureza territorial das consequências em questão evoca uma responsabilidade fundamental e primária das autoridades em nível nacional e, como resultado, também traz à tona o papel primordial das regulamentações para mitigar esses riscos e obter os "melhores resultados nacionais".

10. Mais recentemente, destacados pela pandemia da covid-19 e pelo escrutínio e intervenção adicionais do Estado na infraestrutura de saúde (incluindo pessoal relacionado à saúde, propriedade intelectual, matérias-primas, cadeias de suprimentos, dados etc.), todos sendo designados ou reenfatizados como críticos. Conferir Markopoulou e Papakonstantinou (2021) e Cohen (2010), este último observa que a CI está "impedindo a decadência da sociedade moderna".

11. Conferir Humphreys (2019, p. 2, tradução nossa), que observa que "a consciência da vulnerabilidade potencial da infraestrutura moderna a ataques deliberados ou desastres naturais data pelo menos do período entre guerras, quando os teóricos militares americanos e britânicos especularam pela primeira vez que visar a infraestrutura industrial e o moral civil das potências do eixo com bombardeios estratégicos de longo alcance poderia trazer a vitória a um custo relativamente baixo". Conferir também Biddle (2009) e Zaharia (2012).

estrangeiros que tiveram um efeito profundo no debate em torno da CI. Conforme mencionado anteriormente, essa integração transformou o debate mais técnico, que agora se concentrava principalmente na segurança cibernética.

Vale observar que, concomitantemente ao surgimento de maiores mecanismos de ameaça, também surgiu uma percepção maior de ameaças em resposta a incidentes proeminentes de terrorismo nacional e internacional que ocorreram durante o mesmo período, especialmente (mas não exclusivamente) nos Estados Unidos, cujo ecossistema tem sido um dos principais impulsionadores do campo.[12]

A combinação de ambos os fenômenos (ou seja, o surgimento da segurança cibernética e o aumento da percepção de ameaças estrangeiras) trouxe mais atenção e recursos para o desenvolvimento e o estudo da CI, tanto como prática política quanto como campo de estudo, muitas vezes com ênfase especial na "resiliência" da CI como um subconjunto da segurança de TI (Gritzalis, Theocharidou e Stergiopoulos, 2019; Ganguly, Bhatia e Flynn, 2018; Bologna, 2018). Entretanto, o campo da proteção de CI agora ganhou maior riqueza e diversidade em suas abordagens ao integrar "aspectos organizacionais, gerenciais, sociais, políticos, culturais e humanos" (Gheorghe *et al.*, 2018; Felice e Petrillo, 2018) com profissionais, autoridades e pessoal de sistemas relacionados também interessados em "pesquisa e gestão de operações, economia, análise de risco e gestão de defesa" (Keupp, 2020; Baggett e Stout, 2022; Rass *et al.*, 2020; Verdoodt, 2020).[13]

Em 2008, a OCDE observou que a proteção da CI estava recebendo "atenção especial"[14] nas políticas de investimento estrangeiro de vários países. O debate a seu respeito já havia, portanto, assumido uma dimensão mais pronunciada de segurança econômica, um termo que persistiu e ganhou maior adoção na formulação de políticas nacionais junto com as dimensões de segurança física e cibernética já bem estabelecidas discutidas anteriormente.

Como o termo sugere, dentro dessa esfera, o investimento estrangeiro em CI é visto menos a partir de uma lente baseada no mercado ou no desenvolvimento e mais a partir de uma lente baseada na segurança. Isso não quer dizer que a primeira tenha se tornado menos relevante ou aplicável. De fato, em virtude do seu tamanho e da sua natureza de capital intensivo, os projetos de investimento

12. Incluem-se o atentado à bomba de 1993 contra o World Trade Center em Nova York e o de 1995 em Oklahoma City e os ataques de 11 de setembro de 2001, que "tiveram um efeito galvanizador na política de segurança interna e, por extensão, na proteção da infraestrutura essencial" (Humphreys, 2019, p. 12, tradução nossa). Conferir também Lewis (2020). De fato, algumas das recomendações do relatório da comissão do 11 de setembro estavam explicitamente relacionadas à infraestrutura essencial. Disponível em: https://9-11commission.gov/report/.

13. Para uma visão interdisciplinar no campo dos estudos jurídicos, conferir Vedder *et al*. (2020).

14. Disponível em: www.oecd.org/daf/inv/investment-policy/40700392.pdf. Observa-se o mesmo mais tarde em 2018. Mais informações estão disponíveis em: https://web-archive.oecd.org/2018-11-20/498106-Current-trends-in-OECD-NatSec-policies.pdf.

estrangeiro na CI podem ser justificáveis, uma vez que possuem imenso valor puramente comercial, incluindo valiosos vínculos industriais ou de mercado. Da mesma forma, para o Estado anfitrião, embora não seja de forma alguma garantido, os projetos de investimento estrangeiro em CI também podem ser justificáveis, visto que proporcionam um impacto positivo significativo no desenvolvimento. O investimento estrangeiro em CI não é, portanto, uma atividade incomum ou necessariamente desfavorável, principalmente no mundo em desenvolvimento, em que frequentemente faltam alternativas para fontes de capital e tecnologia.

3.1 Dados críticos

A expansão das noções do que consiste a CI, por sua vez, afetou o escopo dos ISMs e as decisões de triagem. Por exemplo, a pandemia da covid-19 deu maior ênfase aos setores de saúde e cadeia de suprimentos de alimentos como CI, o que, por sua vez, afetou as decisões de ISM relacionadas ao setor. Entretanto, esse fenômeno talvez tenha sido mais profundo no caso de CD, um conjunto de ativos vasto e complexo o suficiente para justificar uma categoria própria. Dentro de CD, embora haja alguma sobreposição, são discerníveis pelo menos três subcategorias que estão sob a alçada da maioria dos ISMs e que, em linhas gerais, podem ser consideradas riscos de boa-fé à segurança nacional, dada a sua relação com o funcionamento de uma economia ou sociedade e a prestação de serviços relacionados às necessidades humanas básicas.

A primeira dessas subcategorias refere-se a dados diretamente relacionados à CI, um reflexo de como o que consiste em CI está agora muito além dos tijolos físicos e da argamassa com os quais é construída.[15] Esses dados geralmente consistem em informações necessárias e geradas para a construção e manutenção da própria CI. Uma segunda subcategoria de CD consiste em dados comerciais e propriedade intelectual, como segredos comerciais de entidades dos setores público e privado envolvidas em negócios relacionados à CI. Finalmente, uma terceira subcategoria discernível de CD consiste em dados pessoais de cidadãos privados, especialmente quando gerados e armazenados em grande escala ou quando pertencem a funcionários de organizações relacionadas à CI.

Distinguir CD de CI é particularmente importante, dado que a amplitude das vulnerabilidades decorrentes dos riscos de segurança de investimentos estrangeiros relacionados a CD é relativamente menos aparente, mas generalizada e, ao mesmo tempo, potencialmente mais difícil de mitigar. Por exemplo,

15. Na Austrália, a Lei de Segurança de Infraestruturas Críticas de 2018 define dados críticos de negócios como: i) informações pessoais relacionadas a pelo menos 20 mil indivíduos; ou ii) informações relacionadas a qualquer pesquisa e desenvolvimento em relação a um ativo de CI; ou iii) informações relacionadas a quaisquer sistemas necessários para operar um ativo de CI; ou iv) informações necessárias para operar um ativo de CI; ou v) informações relacionadas ao gerenciamento de riscos e à continuidade dos negócios (independentemente da descrição) em relação a um ativo de CI.

mesmo com uma participação acionária minoritária, um investidor estrangeiro pode obter acesso ou controle suficiente sobre o CD pertencente à entidade-alvo, por meio do qual esses dados podem ser multiplicados, reproduzidos e armazenados inúmeras vezes a um custo baixo, sem chance de recuperação. Nesse caso, a viabilidade dos recursos disponíveis para desfazer esse dano seria limitada. Isso pode ser comparado ao acesso de um investidor estrangeiro ao controle de CI físico, que poderia ser atenuado com relativa facilidade e os danos resultantes poderiam ser descontinuados, se não desfeitos.

De modo geral, os ISMs lidam com os ativos de CI e de CD de forma semelhante, uma vez que oferecem ao Estado a oportunidade de intervir em transações relacionadas no estágio anterior ao estabelecimento, seja condicionando-as ou, como último recurso, bloqueando-as. Os ativos de CD são frequentemente previstos de forma explícita nos ISMs contemporâneos. O ISM alemão, por exemplo, considera a variedade de *softwares* usados e os dados processados na operação de CI relacionada à energia. De fato, em 2020, a OCDE observou que, nos Estados europeus, estava surgindo uma convergência em termos do tratamento de dados pessoais dentro do escopo das políticas de ISM.

Isso destaca que os dados pessoais e as empresas orientadas por dados são frequentemente o foco especial das decisões do ISM e considerados fontes de riscos à segurança nacional quando adquiridos por investidores estrangeiros. Esses dados, em razão de sua natureza pessoal e de seu vasto tamanho, podem ser potencialmente processados e manipulados para perturbar o funcionamento normal de qualquer sociedade, especialmente as democráticas, nas quais as eleições podem sofrer interferência ao visar tipos específicos de eleitores para manipular suas preferências de voto. Além disso, os dados pessoais podem pertencer a funcionários que estejam conectados à CI. Nos Estados Unidos, por exemplo, um aplicativo móvel de namoro e outro de assistência médica receberam, no passado, um exame minucioso do Committee on Foreign Investment in the United States (CFIUS) – o ISM do país. De fato, o CFIUS e os ISMs de vários Estados-membros da União Europeia (UE) incluem explicitamente dados pessoais em seu escopo.[16]

Além dos ISMs, os Estados têm demonstrado uma tolerância muito baixa em relação à permissão para que entidades estrangeiras, especialmente as

16. O Foreign Investment Risk Review Modernization Act (FIRRMA) de 2018 dos Estados Unidos abrange informações pessoais confidenciais que contêm dados identificáveis ou consistem em um conjunto de dados sobre 1 milhão de indivíduos. Da mesma forma, o regulamento de IED (*foreign direct investment* – FDI) da UE de 2019 identifica o acesso e a capacidade de controlar informações confidenciais, incluindo dados pessoais, como uma consideração importante ao realizar a análise de segurança. Esse regulamento declara que "ao determinar se um investimento estrangeiro direto pode afetar a segurança ou a ordem pública, os Estados-membros e a comissão podem considerar seus possíveis efeitos sobre (a) infraestrutura crítica, física ou virtual, incluindo processamento ou armazenamento de dados e (b) acesso a informações confidenciais, incluindo dados pessoais ou a capacidade de controlar essas informações" (tradução nossa). Disponível em: https://eur-lex.europa.eu/eli/reg/2019/452/oj.

controladas pelo Estado, obtenham acesso ou controle de ativos de CD também por meio de outras formas de trocas internacionais, além das transações tradicionais, como fusões ou aquisições. Em vez disso, *joint ventures*, vendas de ativos e até mesmo colaborações de pesquisa estão cada vez mais no radar das autoridades estatais, seja por meio de seus ISMs ou de outra forma. Isso reflete a natureza precária dos ativos de CD resultante de sua intangibilidade, que permite a ocorrência de um conjunto mais diversificado e dissimulado de mecanismos de ameaça, em comparação com os ativos tangíveis de CI.

3.2 Tecnologias críticas

É claro o que um Estado pode considerar crítico, e, portanto, estar dentro do escopo de um ISM consistiria não apenas em fatores objetivos relacionados às necessidades humanas básicas e ao funcionamento de qualquer sociedade moderna, mas também em fatores subjetivos baseados nas particularidades de um determinado Estado que podem, por exemplo, estar relacionados a fatores históricos, geográficos, geopolíticos ou ideológicos. Novamente, mesmo quando subjetivos, para permanecerem verdadeiramente críticos, esses ativos precisariam, em última instância, estar relacionados ao funcionamento dessa sociedade específica e não apenas à sua competitividade econômica ou liderança global.

É nesse ponto que a conceituação de segurança nacional destacada e oferecida por este texto começa a se diferenciar da prática moderna de ISM, conforme conduzida especialmente no Norte global, onde se um Estado perde competitividade no mercado global para uma determinada tecnologia de ponta, essa perda é afirmada como uma ameaça à segurança nacional desse Estado, mesmo quando ela não deixa nenhum impacto perceptível no funcionamento de sua economia ou sociedade, nem está relacionada à prestação de serviços que atendam às necessidades humanas básicas. Este capítulo classifica essa conceituação duvidosa de segurança nacional em "segurança hegemônica", em que a perda do domínio tecnológico (ou "as joias da coroa") é percebida por um Estado como uma ameaça à sua existência e à sua própria identidade.[17]

Para deixar claro, de forma alguma está implícito que a inclusão de tecnologias avançadas nos ISMs está necessariamente relacionada à competitividade ou à preservação da hegemonia. Pelo contrário, é totalmente plausível e, de fato, perfeitamente demonstrável como uma grande variedade dessas tecnologias é essencial para o funcionamento de uma sociedade e para a prestação de serviços que atendem às necessidades humanas básicas. Isso é especialmente verdadeiro quando certas tecnologias são impulsionadas por CD (como internet das coisas) ou são integradas

17. De fato, a legislação e a política de triagem de investimentos dos Estados Unidos também se concentram em garantir a superioridade tecnológica do Estado, especialmente em tecnologias emergentes e fundamentais definidas de forma ampla, que devem abranger áreas importantes da tecnologia da informação e comunicação (TIC).

a ativos de CI, principalmente equipamentos militares. Portanto, as afirmações de riscos à segurança nacional no contexto das tecnologias geralmente têm mérito.

Em 2020, por exemplo, o ISM alemão bloqueou uma aquisição majoritária da IMST GmbH – uma empresa de tecnologia de rádio e comunicação por satélite – por uma entidade que era de propriedade integral de uma empresa chinesa controlada pelo Estado chamada China Aerospace and Industry Group (Casic). A justificativa era que essa aquisição, se permitida, representaria um risco à segurança nacional da Alemanha, visto que os ativos subjacentes aos quais a transação passaria o acesso e o controle para o Estado chinês eram cruciais para a construção da futura CI alemã, incluindo as redes 5G e 6G.

Entretanto, assim como acontece com os ativos de CI e CD, para que pertençam à segurança nacional de uma forma que não envolva a competitividade econômica, os ativos de CT também devem conter uma qualidade de criticidade semelhante à discutida aqui, ou seja, relacionada ao funcionamento da sociedade. No entanto, isso nem sempre é necessariamente o caso.

Por exemplo, na década de 1980, os Estados Unidos viram surgir exatamente essa conceituação de CT durante o auge da competição tecnológica com o Japão, quando os formuladores de políticas norte-americanos iniciaram o que ficou conhecido como "movimento de tecnologias críticas" (Wagner e Popper, 2003). Com esse esforço, os formuladores adotaram o termo *critical*, não para demarcar as tecnologias que eram necessárias para preservar ou manter o funcionamento normal da sociedade, mas para designar aquelas em que se buscava obter vantagem competitiva de pioneiro, como semicondutores e telecomunicações. O objetivo não era defender a segurança nacional, como já conceituado, mas sim consolidar um domínio global de longo prazo sobre essas tecnologias.

Além da conceituação hegemônica, o que é mais desafiador no contexto da CT é quando se consideram as tecnologias de "uso duplo". Esses ativos, por definição, pertencem simultaneamente a aplicações militares e civis. Como resultado dessa dualidade, torna-se difícil desvincular sua criticidade de seu uso puramente comercial, que deve ser tratado caso a caso.

4 O CARÁTER DISTINTIVO DA CRITICIDADE

As escolhas terminológicas são muito importantes na formulação de políticas e nos debates acadêmicos, principalmente no contexto dos ISMs, em que a forma como escolhemos designar os ativos econômicos que devem ser transacionados tem grande impacto sobre a quantidade e o tipo de atenção que os ativos recebem, bem como sobre as ações necessárias para essa transação. As decisões sobre ISM, por sua vez, têm um efeito significativo na segurança nacional e no ambiente econômico e político de um Estado.

Conforme observado anteriormente, não é coincidência o fato de o termo crítico, que se originou e evoluiu de forma mais vívida no campo da proteção de CI e de estudos de segurança mais amplos, ter sido cada vez mais utilizado nas regras de ISM. Isso é especialmente verdadeiro, pois tanto a proteção de CI quanto os ISMs têm um objetivo subjacente comum de salvaguardar a segurança nacional, sendo que o segundo teve seu auge muito depois que o primeiro já havia amadurecido como campo de estudo e área de política. Isso é uma sorte, uma vez que a criticidade como conceito é um termo adequado, na verdade o mais adequado, para a formulação de políticas de ISM, não apenas por causa das metas comuns compartilhadas pelos ISMs e pela proteção de CI, mas também porque a criticidade tem uma base técnica e objetiva que nos permite filtrar, pelo menos algumas, afirmações de segurança nacional que não têm justificativa suficiente ou são falsas.

O argumento central dessa contribuição, no entanto, vai um passo além, ou seja, não só o termo crítico contém um filtro apropriado embutido, mas também outros termos (como estratégio ou sensível) que são usados com frequência para designar os mesmos ativos e utilizados muitas vezes de forma intercambiável com crítico não possuem essa qualidade técnica. Portanto, embora possam continuar a ser utilizados no contexto dos ISMs em conjunto com crítico, eles não devem ser considerados intercambiáveis. A criticidade, conforme conceituada aqui, é uma propriedade específica amplamente objetiva e distinta de valor estratégico ou sensibilidade, que são propriedades cujos significados são relativamente vagos, subjetivos e não técnicos. Como resultado, ao contrário de crítico, eles não oferecem nenhum apoio ao objetivo de determinar quais afirmações de segurança nacional são empiricamente sólidas.

Para deixar claro, não se sugere que a criticidade como uma lente seja autossuficiente para o propósito de avaliar as reivindicações de segurança nacional nos termos dos ISMs. Entretanto, ela é de fato um ponto de partida fundamental, especialmente para o escopo dos ISMs. Uma vez estabelecida a criticidade, também seria necessário verificar qual a vulnerabilidade específica que surgiria de uma determinada transação, se essa vulnerabilidade poderia ser mitigada e, caso contrário, com base em que o investidor estrangeiro não pode ser considerado confiável o suficiente para se abster de tirar proveito dessa vulnerabilidade. Essas discussões, no entanto, estão além do escopo deste texto.

Por enquanto, afirmamos que criticidade fornece um padrão de base importante e subestimado, por meio do qual não só é possível distinguir afirmações de segurança nacional empiricamente sólidas de afirmações implausíveis, mas também quais dessas afirmações são realmente hegemonicamente orientadas, ou seja, mais sobre domínio tecnológico e liderança econômica. A filtragem por criticidade,

portanto, também é um lembrete claro de que a noção de riscos à segurança nacional decorrentes de investimentos estrangeiros internos não é plausível apenas para economias avançadas, desenvolvidas e potências dominantes, mas também para Estados em desenvolvimento e potências médias, dado que os ativos de CI e CD, ou mais especificamente as vulnerabilidades que eles podem acarretar, também existem na última categoria.

5 CONSIDERAÇÕES FINAIS

Embora o recente aumento dos ISMs possa ter se concentrado no Norte global e tenha sido impulsionado principalmente pela resposta aos investimentos controlados pelo Estado e originários da República Popular da China, a análise apresentada aqui fornece evidências teóricas de que o problema da segurança nacional no contexto do investimento estrangeiro, com a criticidade em seu cerne, é, no entanto, universalmente aplicável na medida em que os ativos de CI e CD são predominantes em todo o mundo, além da divisão Norte-Sul.

Independentemente da posição normativa que um Estado decida adotar e do investidor estrangeiro que considere suficientemente confiável, enquanto certas necessidades básicas da sociedade permanecerem constantes, os ativos econômicos (e os dados relacionados) que facilitam seu fornecimento se manterão essenciais. Portanto, o acesso ou o controle de tais ativos por entidades estrangeiras, especialmente as controladas pelo Estado, continuaria sendo uma questão plausível de segurança nacional. Se transações específicas devem ou não ser bloqueadas, condicionadas ou permitidas, conforme proposto originalmente, continua sendo uma questão separada a ser verificada caso a caso.

Adotar a criticidade como uma lente analítica nos permite aprimorar nossos entendimentos conceituais de segurança nacional e começar a desvendar as afirmações sobre ela no contexto do investimento estrangeiro. É também um lembrete da natureza interdisciplinar do campo e de como a análise apenas das normas jurídicas em sua forma de letra preta, sem apreciar as origens técnicas da terminologia que elas adotam, inevitavelmente levará a respostas insuficientes.

REFERÊNCIAS

BAGGETT, R.; STOUT, A. Critical infrastructure risk analysis and management. *In*: MASYS, A. (Ed.). **Handbook of security science**. Cham: Springer, 2022. Disponível em: doi.org/10.1007/978-3-319-51761-2_1-1.

BIDDLE, T. **Rhetoric and reality in air warfare**: the evolution of British and American ideas about strategic bombing, 1914-1945. New Jersey: Princeton University Press, 2009.

BOLOGNA, S. Cybersecurity of critical infrastructures. *In*: MASYS, A. (Ed.). **Handbook of security science**. Cham: Springer, 2018.

COHEN, F. What makes critical infrastructures critical? **International Journal of Critical Infrastructure Protection**, v. 3, n. 2, p. 53-54, 2010. Disponível em: https://www.researchgate.net/publication/245480861_What_makes_critical_infrastructures_Critical.

DIMITROPOULOS, G. National security: the role of investment screening mechanisms. *In*: CHAISSE, J.; CHOUKROUNE, L.; JUSOH, S. (Ed.). **Handbook of international investment law and policy**. Singapore: Springer, 2020. Disponível em: https://doi.org/10.1007/978-981-13-5744-2_59-1.

FELICE, F.; PETRILLO, A. **Human factors and reliability engineering for safety and security in critical infrastructures**: decision making, theory, and practice. Cham: Springer, 2018.

FIRB – FOREIGN INVESTMENT REVIEW BOARD. **Australia's foreign investment policy**. [s.l.]: Treasury/Australian Government, Jan. 2021. (Guidance Note).

GALLAIS, C.; FILIOL, E. Critical infrastructure: where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure. **Journal of Information Warfare**, v. 16, n.1, p. 64-87, 2017.

GANGULY, A.; BHATIA, U.; FLYNN, S. **Critical infrastructures resilience**: policy and engineering principles. London: Routledge, 2018. Disponível em: https://doi.org/10.4324/9781315153049.

GHEORGHE, A. *et al*. **Critical infrastructures, key resources, key assets**: risk, vulnerability, resilience, fragility, and perception governance. [s.l.]: Springer, 2018.

GRITZALIS, D.; THEOCHARIDOU, M.; STERGIOPOULOS, G. **Critical infrastructure security and resilience**: theories, methods, tools and technologies. 1st ed. [s.l.]: SpringerLink, 2019. 313 p. Disponível em: https://lib.ugent.be/catalog/ebk01:4100000007334920.

HUMPHREYS, B. E. **Critical infrastructure**: emerging trends and policy considerations for Congress. [s.l.]: CRS, 2019.

KEUPP, M. The security of critical infrastructures: introduction and overview. *In*: _____. (Ed.). **The security of critical infrastructures**, [s.l.]: Springer, 2020. p. 1-14. (International Series in Operations Research and Management Science).

KONG, T. Y.; LI, Y. **China's new national security screening rules on foreign investment**. [s.l.]: EAI/NUS, 4 Feb. 2021. (EAI Commentary, n. 24). Disponível em: research.nus.edu.sg/eai/wp-content/uploads/sites/2/2021/02/EAIC-24-20210204-1.pdf.

LEWIS, T. G. **Critical infrastructure protection in homeland security**: defending a networked nation. 3rd ed. Hoboken: Wiley, 2020.

MARKOPOULOU, D.; PAPAKONSTANTINOU, V. The regulatory framework for the protection of critical infrastructures against cyberthreats: identifying shortcomings and addressing future challenges – the case of the health sector in particular. **Computer Law and Security Review**, v. 41, 2021. Disponível em: https://ssrn.com/abstract=3979511.

MISRA, M. Foreign investment in Critical National Infrastructure (CNI) by State-Controlled Entities (SCEs) and Investment Screening Mechanisms (ISMs). *In*: DELIMATSIS, P.; DIMITROPOULOS, G.; GOURGOURINIS, A. (Ed.). **State capitalism and International Investment Law**. [s.l.]: Bloomsbury, 2023.

RASS, S. *et al*. **Cyber-security in critical infrastructures**: a game-theoretic approach. Cham: Springer, 2020. Disponível em: https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Cyber-Security%20in%20Critical%20Infrastructures.pdf.

UNCTAD – UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **World investment report 2016**: investor nationality – policy challenges. Geneva: UN, 2016. Disponível em: https://unctad.org/system/files/official-document/wir2016_en.pdf.

_____. Recent policy developments and key issues. *In*: UNCTAD – UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **World investment report 2018**: investment and new industrial policies. Geneva: UN, 2018. Chap. 3, p. 79-124. Disponível em: https://unctad.org/system/files/official-document/wir2018ch3_en.pdf.

UNITED KINGDOM. **Strategic framework and policy statement on improving the resilience of critical infrastructure to disruption from natural hazards**. London: Cabinet Office, 2010.

VEDDER, A. *et al*. **Security and law**: legal and ethical aspects of public security, cyber security and critical infrastructure security. Antwerpen: Intersentia, 2020. Disponível em: https://lib.ugent.be/en/catalog/rug01:002793333.

VERDOODT, V. **Children's rights and commercial communication in the digital era**: towards an empowering regulatory framework for commercial communication. Cambridge: Intersentia, 2020. (KU Leuven Centre For IT and IP Law Series).

WAGNER, C.; POPPER, S. Identifying critical technologies in the United States: a review of the federal effort. **Journal of Forecasting**, v. 22, n. 2/3, p. 113-128, 2003. Disponível em: https://doi.org/10.1002/for.854.

WEHRLÉ, F.; POHL, J. **Investment policies related to national security**: a survey of country practices. Paris: OECD Publishing, 2016. (OECD Working Papers on International Investment, n. 2016/02). Disponível em: https://doi.org/10.1787/5jlwrrf038nx-en.

ZAHARIA, A. **"Critical infrastructure" concept's evolution and prospects within the euro-atlantic framework**. Bucharest: Carol I National Defence University, 2012. p. 59-72. Disponível em: https://www.proquest.com/scholarly-journals/critical-infrastructure-concepts-evolution/docview/1291938718/se-2.