L'implementazione delle *smart grid* come paradigma della Sicurezza Nazionale: potenziale *vulnus* o elemento imprescindibile del Sistema Paese?

Ten. Lorenzo Mina & Matteo Negro

Le reti intelligenti, o smart grid*, sono le protagoniste della rivoluzione energetica e digitale che l'Italia sta portando avanti all'interno del piano di ammodernamento di settori critici, quali le infrastrutture di distribuzione energetica, le reti digitali e i sistemi informatici ad esse collegati. L'autosufficienza energetica, la tutela delle infrastrutture critiche e la protezione delle reti si configurano come elementi imprescindibili del meccanismo di difesa del Sistema Paese. Questo contributo mira a fornire una panoramica dell'argomento, non solo descrivendo i vantaggi conseguenti all'impiego dei sistemi di distribuzione intelligenti, ma anche le possibili vulnerabilità che una conoscenza non adeguata del tema può comportare. In particolare, saranno sottolineate le potenziali minacce che la digitalizzazione dell'infrastruttura energetica può far emergere, specialmente nei casi in cui la stessa asserva installazioni critiche. La discussione procederà all'analisi dei benefici con un approccio omnicomprensivo finalizzato all'analisi dell'intero sistema modale. Per ultimo, particolare attenzione sarà posta a casi specifici d'interesse come il concetto di* Smart Military Districts *o i risvolti strategici, di efficientamento energetico e di transizione ecologica che l'utilizzo delle reti intelligenti comporta.*

Introduzione

Le reti elettriche intelligenti, o *smart grid*, rappresentano l'evoluzione dell'infrastruttura di distribuzione energetica, integrando le tecnologie di informazione e comunicazione (ITCs)[1] alla rete tradizionale, permettendo quindi il passaggio dalla struttura standard unidirezionale al network intelligente bidirezionale e integrato. Questa evoluzione è risultata necessaria in seguito alla crescita esponenziale della domanda di energia globale, dell'uso e della diffusione delle fonti rinnovabili e dell'integrazione delle nuove

[1] *Information and communications technologies* (ICTs).

tecnologie, tra cui figurano oltre le ITCs anche le nuove tecnologie di misura energetica (*smart metering*) sia in generale le cosiddette *Emerging & Disruptive Technologies* (EDTs)[2], di cui le ITCs fanno anch'esse parte. In questo senso sarà comprensibile la grande attenzione e curiosità che suscita l'implementazione di queste innovazioni, processo già in atto e imprescindibile, che coinvolge differenti attori e differenti livelli operativi, dal singolo utente/consumatore privato a entità nazionali, regionali e sovra-nazionali, e nella sua dimensione sistemica, risulta una delle maggiori grandi opere che il Paese sta attualmente sviluppando.

Nel caso delle *smart grid*, vi sono già piani di implementazione per quanto riguarda l'Italia e le due più importanti entità sovra-nazionali di cui fa parte, Unione Europea (UE)[3] e Alleanza Nordatlantica (NATO)[4]. Una più elaborata analisi dei risvolti dell'applicazione di questa tecnologia diviene quindi necessaria assumendo il punto di vista del Sistema Paese, esaminando le infinite possibilità e i vantaggi che questa comporta e prevenendo immediatamente le possibili criticità e vulnerabilità che una pianificazione non attenta può comportare. Questo breve approfondimento sarà altresì influenzato dall'attuale situazione pandemica; i recenti avvenimenti hanno infatti non solo accelerato il processo di digitalizzazione già in atto, ma possono inoltre facilitare un pensiero intorno nuovi campi d'applicazione difficilmente identificabili in precedenza. Oltre a ciò, rendono palese il vantaggio e la potenzialità di questa tecnologia applicate a qualsiasi campo pubblico, non solo industriale-logistico-produttivo-infrastrutturale-militare come una prima corrente di pensiero pareva supporre, ma anche economico-finanziario, amministrativo e specialmente sanitario. Infine, fondamentale è il contributo che le *smart grid* possono

[2] Cf. anche Dotoli, Pierpaolo. "Tecnologie Emergenti e possibili impieghi futuri in campo militare: Le prospettive internazionali". CASD, Ce.Mi.S.S., 2014.

[3] cf. per esempio, EC Directorate-General for Energy 2011, SETIS 2014 e EC 2014 su Smart Metering.

[4] Relativamente a questioni di protezione e strategia energetica Nord-Atlantica cf. per esempio, comma 78 in Brussels Summit Declaration 2018, comma 52 in Chicago Summit Declaration 2012 e comma 48 in Bucharest Summit Declaration 2008.

apportare alla Difesa nazionale[5], specialmente in ambito di sicurezza energetica[6] e di indipendenza da infrastrutture esterne, soddisfacendo il consolidato paradigma *energy security*-cybersecurity.

Potenziali vulnera dell'impiego della tecnologia smart nelle reti infrastrutturali energetiche

Le preoccupazioni maggiori per quanto riguarda la sicurezza delle *smart grid* riguardano principalmente l'aspetto digitale della tecnologia, ovvero il flusso di dati e i software impiegati. Ad essi, si deve sommare la possibilità dell'errore umano involontario, che può avvenire con più frequenza rispetto all'infrastruttura tradizionale visto il maggior numero di compiti gestionali e di controllo che questa tecnologia richiede, unitamente a una formazione più specialistica, tecnica e interdisciplinare.

I *vulnera* sistematici principali sono abitualmente riassunti dalla letteratura[7] in tre punti, il cui soddisfacimento risulta imprescindibile per il corretto funzionamento della rete. In primo luogo, è necessario garantire l'integrità sistemica della rete, prevenendo eventuali possibilità di alterazione, modifica, creazione o distruzione di dati e informazioni. Salvaguardata la rete, risulta quindi essenziale assicurare la confidenzialità delle informazioni e dei dati conservati nella stessa. Per ultimo, la possibilità di accesso alla rete da parte dei gestori, degli utilizzatori e dei produttori deve risultare continuo, costante e veloce.

Oltre a queste vulnerabilità piuttosto generali, derivate non tanto da caratteristiche particolari delle *smart grid* quanto dall'implementazione dell'infrastruttura ICT all'interno di una rete energetica tradizionale, altre preoccupazioni più specifiche sono

---

[5] cf. *Scenari Futuri*, SMD 2021 o Dotoli. "Tecnologie Emergenti e possibili impieghi futuri in campo militare: Le prospettive internazionali".

[6] cf. Relazione sulla politica dell'informazione per la sicurezza 2020, SISR, (2021)

[7] Dupuy, Arnold, et al.. "Energy Security in the Era of Hybrid Warfare", *Nato Review*, 2021. https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html or Aloul, Fadi, et al.. "Smart Grid Security: Threats, Vulnerabilities and Solutions." *International Journal of Smart Grid and Clean Energy*, 2012, 1–6. doi:10.12720/SGCE.1.1.1-6.

sorte[8]. Rispetto l'infrastruttura tradizionale, la sicurezza fisica di una rete *smart* si rivela più complessa e difficoltosa, in quanto i differenti nodi ed elementi della rete risultano variamente distribuiti e capillarmente diffusi sul territorio, anche al di fuori di aree protette e controllabili. Oltre a ciò, la vita energetica dei singoli elementi può comportare l'emergere di criticità nella misura in cui i componenti diventano obsoleti e le capacità funzionali degli stessi si riducono. Questo processo risulta drasticamente più veloce e di maggior portata se comparato alla possibilità di elementi obsoleti in una rete tradizionale e rende necessario una particolare attenzione all'eventuale sostituzione di elementi hardware obsoleti al fine di garantire la salvaguardia del sistema. Relativamente a queste due aree problematiche appena evidenziate, emerge allo stesso modo la problematica riguardante l'alto numero di componentistica che una rete *smart* richiede e le conseguenti capacità gestionali, amministrative e operative che la salvaguardia e la protezione degli stessi richiedono. La stessa componentistica *smart* presenta un'ultima problematica intrinseca: una rete *smart* è definita come tale anche in virtù della cosiddetta fiducia implicita degli elementi costituenti, ovvero la caratteristica che permette l'interrelazione dei differenti nodi, cioè delle singole unità hardware in grado di comunicare con le altre unità della rete. Nel caso un nodo venga attaccato e compromesso, i dati manipolati o corrotti verrebbero inviati ed accettati dai nodi ad esso correlati, senza essere in grado di valutarne l'affidabilità. Infine, la presenza di *stakeholder* multipli all'interno del sistema può causare l'emergere di problematicità relativamente ai differenti attori e/o portatori d'interesse che influenzano, gestiscono o controllano la rete *smart*; in questo senso è utile richiamare apporti da altre discipline, come l'impiego normativo del *Golden Power* a tutela di settori e industrie chiave del Sistema Paese o il più recente complesso legislativo del Perimetro di Sicurezza Nazionale Cibernetica[9].

[8] Aloul, 'Smart Grid Security: Threats, Vulnerabilities and Solutions'; Jokar, Paria, Nasim, Arianpoo and Victor C. M. Leung. "A survey on security issues in smart grids." *Secur. Commun. Networks* 9 (2016): 262-273.

[9] Cfr. d.l. 34/2020 (cd. decreto Rilancio, art. 240) e d.l. n. 105 del 2019/n. 162 del 2019 e conseguente DPCM 30 luglio 2020, n. 131 (G.U. 21 ottobre 2020, n. 261).

In pratica, queste vulnerabilità implicite del sistema possono portare ad attacchi informatici diretti alla componentistica[10], ai protocolli informatici[11] o alla topologia[12] della rete, con l'utilizzo di malware indirizzati ai server intelligenti, accessi criminali ai database di controllo, attacchi all'infrastruttura comunicativa informatica[13], attacchi *replay*[14], attacchi alle suite di protocolli Internet[15], intercettazioni del traffico di dati, attacchi indirizzati al protocollo Modbus del sistema SCADA[16] e differenti modalità di *data exploit*[17,18].

Soprattutto, la rete intelligente integrata può drasticamente aumentare il rapporto di asimmetricità del conflitto energetico[19], in quanto il sistema digitale integrato permetterebbe anche a entità singole o gruppi di piccole dimensioni di effettuare attacchi ostili verso entità statali o sovra-statali. Oltre a ciò, assumendo la prospettiva di un conflitto tra entità nazionali, la rete *smart* risulterebbe un possibile *vulnus* fondamentale all'interno del conflitto, la cui protezione e salvaguardia diverrebbero fondamentale per evitare una crescita esponenziale del rapporto di forza conflittuale per la parte avversa, nel caso essa risulti capace di impossessarsi, accedere o assumere in qualsiasi modo il controllo della rete o dei sistemi di controlli digitale del Paese attaccato.

---

[10] *Remote Terminal Units* (RTUs).

[11] Ingegneria inversa e inquinamento con falsi dati.

[12] Attacchi DoS e limitazione delle capacità gestionali e preventive.

[13] Sia con scopi di danneggiamento immediato sia con la creazione di backdoor dormienti per attacchi futuri.

[14] Oltre che con finalità di controllo e manipolazione dei data pack.

[15] TCP/IP stack.

[16] *Supervisory Control And Data Acquisition.*

[17] Ad esempio, produzione di intelligence conseguente alla lettura dei dati di utilizzo dei sistemi.

[18] Aloul, 'Smart Grid Security: Threats, Vulnerabilities and Solutions'. Cf. anche Butun, Ismail, Alexios Lekidis and dos Santos, Daniel Ricardo. "Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities." ICISSP (2020) relativamente alle vulnerabilità dei protocolli e del sistema informatico.

[19] Relativamente al concetto di conflitto asimmetrico cf. anche Cucchini Ruggero, Ruzza, Stefano. "Asimmetria e trasformazione della guerra. Spazio, tempo ed energia nel nuovo contesto bellico", in ID Informazioni della Difesa (2007): 32-37

Benefici derivati dall'impiego della tecnologia intelligenti all'interno delle reti infrastrutturali energetiche

Il discorso intorno alle criticità e le vulnerabilità delle *smart grid* dev'essere intrapreso non solo per prevenire al meglio possibili problematiche della sicurezza, quanto per sfruttare al meglio le potenzialità della tecnologia intelligente e i suoi vasti campi d'applicazione; tra queste spiccano i benefici diretti derivati dall'impiego della tecnologia, i benefici derivati dall'interconnessione sistemica dei vari attori coinvolti, i benefici particolari inerenti specifici settori chiusi e la relazione tra gli stessi ed infine i benefici sistemici derivati dall'impiego della tecnologia intelligente in ambito regionale e sovra-nazionale, i quali influenzano anche benefici e ricadute politiche nei Paesi coinvolti.

La rete *smart* provvede a garantire maggiore equità, sicurezza sistemica e rottura dell'integrazione verticale di distribuzione. Le singole celle giovano dell'impiego della tecnologia *smart* sia nella riduzione dei consumi, nell'aumento della capacità gestionale e di controllo e nella possibilità di utilizzo di fonti rinnovabili/alternative, sia nel contrasto a sprechi infrastrutturali e possibili attività illegali (appropriazione indebita, allaccio abusivo, furto di energia). Questo sistema riesce a garantire un mercato aperto i cui nodi principali risultano al contempo slegati gli uni dall'altro e pienamente integrati nella struttura, favorendo la distribuzione e l'autosufficienza energetica anche in situazione nodali critiche in cui la fornitura può risultare interrotta in un determinato punto del sistema. Assumendo una prospettiva nazionale o sovra-nazionale di collegamento infrastrutturale questi stessi benefici sono altresì validi in caso di contrazione critica della fornitura energetica a livello nazionale e/o regionale, anche in caso di possibile atto ostile e destabilizzante portato avanti da attori nemici e/o gruppi terroristici. Oltre ai benefici singoli e sistemici, diversi settori specifici possono giovare di benefici particolari derivati dall'implementazione delle *smart grid* all'interno del proprio sistema. Tra questi, esempio per eccellenza è lo *Smart Military District*, ovvero un distretto militare strategico autosufficiente e intelligente, già in sviluppo e

fondamento della strategia energetica nazionale e internazionali[20]. Oltre al distretto militare strategico, tutti i settori pubblici ne risentirebbero favorevolmente: il settore sanitario, la pubblica sicurezza, la gestione delle carceri, il settore logistico intermodale e la pubblica amministrazione. Per ultimo, differenti piani di implementazione di possibili *super-grid* future continentali o ultra-continentali vengono abitualmente discussi; tra queste, la *North Seas Countries Offshore Grid Initiative* (NSCOGI), la *Medgrid*, la *European Super Grid* e la *Synchronous Grid of Continental Europe* (ex-UCTE grid), tutte ipotesi o progetti di grid tradizionali eventualmente integrabili con tecnologia Smart (cf. *SuperSmart Grid* - SSG[21]). Questi progetti non solo garantirebbero incredibili benefici infrastrutturali ed energetici (specialmente nell'ambito della gestione, del trasporto e del consumo dell'energia prodotta da fonti rinnovabili, la cui produzione e distribuzione risulta asimmetrica e influenzata da caratteristiche ambientali e geografiche) ma possono risultare utili investimenti statali e sovra-statali con forti ritorni politici e finanziari. Oltre a questo, dal punto di vista della sicurezza energetica, questi progetti garantirebbero una forte autosufficienza energetica, una minore dipendenza dalle importazioni e una difesa da possibili criticità nella fornitura e nella generazione elettrica nei paesi in aree a rischio.

Conclusioni

L'impiego capillare delle *smart grid* appare una fonte necessaria e fondamentale dello sviluppo futuro del Sistema Paese, specialmente tenendo conto delle chiare direttive nazionali ed europee relative alla transizione energetica e ai benefici che la tecnologia *smart* può comportare. Il minor spreco energetico, la più efficiente gestione e distribuzione e le possibilità di impiego diffuso di energie rinnovabili vanno di pari passo con la transizione digitale, sostenibile e verde. Oltre a questo, è interessante sottolineare il paradosso della sicurezza che la tecnologia *smart* sembrerebbe porre:

[20] cf. Audizione del Ministro per la Difesa sulle linee programmatiche del Dicastero presso le Commissioni congiunte 4ª (Difesa) del Senato della Repubblica e IV (Difesa) della Camera dei deputati Roma, 26 luglio 2018.

[21] Battaglini, Antonella, et al., "The SuperSmart Grid", *European Climate Forum,* Potsdam Institute for Climate Impact Research, 2008.

nonostante la maggior parte delle criticità e delle vulnerabilità tradizionali della rete energetica possano essere ridotte o risolte dalle reti intelligenti, nuove problematiche e *vulnera* emergono, relativamente alla digitalizzazione di questo settore chiave. Tuttavia, più che essere rischi intrinsechi di questa tecnologia, essi si inseriscono nel più generale discorso sulla transizione digitale e i rischi che ne conseguono, ed è necessario ricordare come ad un investimento verso le tecnologie energetiche *smart* debba corrispondere un'adeguata attenzione alla formazione in ambito digitale e di cybersecurity. Infine, questo breve contributo si è focalizzato sull'implementazione della rete *smart* in ambito nazionale e comunitario, considerando questa nuova infrastruttura energetica sistemica una grande opera civile e pubblica. Tuttavia, altri ambiti di indagine sorgono, ed è utile sottolineare il possibile impiego di questa tecnologia anche in ambiti nazionali esteri, come all'interno di basi militari estere e di strutture di supporto a operazioni nazionali e internazionali, unendo ai benefici già elencati una forte riduzione dell'impronta logistica militare e, conseguentemente, un minor rischio operativo per l'apparato militare, civile e diplomatico al di fuori dei confini nazionali.

Il Ten. Lorenzo Mina è Ufficiale dell'Arma delle Trasmissioni, in servizio presso il Comando per la Formazione e Scuola di Applicazione dell'Esercito in Torino. Ha frequentato la Scuola Navale Militare "Francesco Morosini" di Venezia (2013-2016). Ha frequentato il 198° Corso "Saldezza" presso l'Accademia Militare di Modena (2016-2018) e si è laureato in Scienze Strategiche presso l'Università degli Studi di Torino con una relazione di laurea dal titolo "Il segreto di Stato", incentrata sulle modifiche apportate dalla legge n. 124/2007. All'interno del suo percorso formativo ha acquisito gli elementi fondamentali in materia di Cybersecurity e Cyber Defense e sviluppato interesse per il ruolo strategico che queste materie avranno nello sviluppo infrastrutturale del Paese. Ha partecipato a molteplici eventi di scambio internazionale nell'ambito della European initiative for the exchange of young officers inspired by Erasmus, tra i quali si evidenziano un modulo presso la Theresian Military Academy austriaca e un modulo organizzato dall'European Security and Defence College a tema

Common Security and Defence Policy. Ha partecipato inoltre alla 19th Competition for military academies sulla Law of armed conflict organizzata dall'International institute of humanitarian law con sede a Sanremo.

MATTEO NEGRO è attualmente studente del corso di laurea magistrale in International Relations, major in Security, presso l'università LUISS "Guido Carli" di Roma. Ex-allievo della Scuola Navale Militare "Francesco Morosini" di Venezia è laureato con lode in Filosofia presso l'università "La Sapienza" di Roma e ha frequentato corsi addizionali presso la facoltà di Giurisprudenza e la facoltà di Scienze Politiche dell'università di Padova. Tra i suoi interessi principali di ricerca figurano l'antropologia politica e legale, l'antropologia delle infrastrutture e l'antropologia linguistica. È membro dell'American Anthropological Association e fa parte del comitato scientifico della Fondazione Dell'Agata. È stato in precedenza borsista della Scuola di Alta Formazione Politica della Fondazione Magna Carta e presidente della sezione giovani dell'Accademia Angelico-Costantiniana.
