Um estudo sobre métodos de pesquisa utilizados em segurança computacional – Criptografia

Vinicius Gadis Ribeiro
vribeiro@inf.ufrgs.br
Professor Adjunto da ULBRA e UNILASALLE*
Doutorando Computação (PPGC-UFRGS)
Membro do GSeg/UFRGS

Universidade Federal do Rio Grande do Sul - Instituto de Informática
Av. Bento Gonçalves, 9500 - Bloco IV
Bairro Agronomia
CEP 91.509-900
Caixa Postal 15.064 - 91.501-970
Porto Alegre - RS - BRASIL

Com o intuito de identificar a maior ocorrência de algum método de pesquisa empregado em pesquisas na área de segurança computacional – em especial, na criptografia – procedeu-se a análise de 952 artigos publicados em eventos internacionais, buscando identificar características de pesquisa que fossem relevantes. Outros aspectos procuraram identificar se a área geográfica influenciaria a metodologia, ou se o tempo influenciaria a metodologia.Observou-se que alguns temas de pesquisa tiveram maior ênfase – uma vez que se gerou, posteriormente, diversos trabalhos sobre aquele tema em outros; ademais, observou-se alguma relação entre o modo de explicitar o método empregado e alguns métodos – como a experimentação e a demonstração matemática. Há a grande produção de alguns países e de instituições nessa área. Alguns países destacam-se líderes em diversos temas e métodos de pesquisa, e alguns têm destaque apenas a esforços nacionais. Ademais, há métodos bastante relacionados com determinados tipos de métodos de pesquisa.

Palavras-chave: Métodos de pesquisa, Criptografia, Segurança computacional, Pesquisa, Enquetes.

---

* Parcialmente patrocinado pelo Centro Universitário LaSalle - UNILASALLE -, e pela Universidade Luterana do

Abstract: *In order to identify tal of occurrence of some research used in search of computing secuspecially in cryptography, 952 arti blished in international showcasalyzed to identify relevant researc Others aspects of interest were tohether geographic area would af method, or whether the time couldnethod. It was observed that some g of research had obtained more inuse it had generated, afterwards, works about that theme than other, it was observed some reaction t the show of the method and someuch as mathematics experimentat demonstration, and big productiocountries and of some institution: area. Some countries had become bme themes and research methods of them ocurring for national effoise, some methods have high relat with some kinds of research meth*

Keywords: *Research methods, by, Computer security, Survey resea*

O atual modelo de produção em como maior prioridade a prc dessa produção através de artigos em eventos científicos, o qual referendados por sua qualidade am corpo editorial.

Não há uma forma explícita de orma como foi produzido o conhec do trabalho de pesquisa. Contudo, o convencional para artigos científ Ciência da Computação inclui, trante, os seguintes elementos [23]:

1. trabalho descreve uma nova iorototipada em um pequeno sistem
2. trabalho alega o seu lugar nalizando comparações de caracterí ou seja, o relatório apresenta uma acterísticas, e compara qualitativa antigas abordagens com a nova, ca a característica.

Tal artigo poderia ser conside atório, se vem a apresentar um realmente radical, ou uma quebrigma. Talvez, quando pela prime se realizou um experimento usanao se propor um Navegador *Web*, havido essa mudança ou descober

Não obstante, não é o que se obudar os tipos de métodos de pesqu contramos, muitas vezes, artigos sentação teórica, sem a definição de m de pesquisa, e diversos outros probcorpo editorial dos anais de evento cada artigo publicado verificasse e n empregada, poder-se-ia obter tra com maior rigor e maior qualidade oppen [8] destaca a relevância de d o método empregado em pesquisando-os nos artigos publicados.

O presente trabalho apresenta o resultado de uma pesquisa *survey* realizada em fins do segundo semestre de 2000, onde os objetos de pesquisa foram artigos publicados em eventos internacionais de Criptografia, que dispunham de corpo editorial. O objetivo de tal estudo foi identificar os tipos de métodos de pesquisa empregados nessa área, além de verificar a existência ou não de correlações geográficas ou temporais, com relação ao método empregado.

Esse estudo encontra-se organizado da seguinte forma: a seção 2 apresenta a metodologia geral da pesquisa, deixando para a seção 3 a descrição de diversos métodos de pesquisa, tradicionalmente empregados nas Ciências. A seção 4 apresenta o método empregado no presente trabalho, bem como os resultados das análises dos dados obtidos. Na última seção, algumas considerações finais e recomendações para trabalhos futuros são apresentadas.

Métodos de Pesquisa

A presente seção apresenta a metodologia geral da pesquisa, os tipos de métodos tradicionalmente aplicados em Ciências, e os tipos de métodos que recentemente têm tido mais progressos, graças ao advento dos computadores, de modo genérico. Aspectos particulares de cada um dos métodos mais utilizados – os chamados tradicionais – serão apresentados em capítulo posterior.

Metodologia Geral da Pesquisa

O trabalho científico inicia com uma pergunta a ser respondida, um problema, uma questão de pesquisa. Há uma dúvida, uma questão, um problema a ser resolvido [KER 79].

Segue-se a necessidade de haver uma idéia que a justifique. Talvez, um conceito a ser definido. Em muitos casos, usa-se ou cria-se um construto [8]. Para garantir a isenção e buscar o veracidade dentro do possível, usa-se de toda uma formalização da pesquisa – pois parte-se do princípio (de modo geral) que outros investigadores, dadas as mesmas condições, poderiam repetir tais formalismos, buscando obter resultados semelhantes. Para a formalização de uma pesquisa, faz-se uso de métodos. O método a ser utilizado depende do tipo de pesquisa, conforme será visto adiante.

Diversos autores buscam formalizar o próprio procedimento de pesquisar, decompondo o processo em fases, e interligando essas fases. Essa ação facilita o processo de ilustrar graficamente todo o processo de pesquisa, possibilitando uma visualização mais adequada de todo o processo.

Na realidade, o a vir influenciar todo o processo de condução sa; uma intervenç todo o formalismo de uma pesquisa por eno contrapartida, dev claro e evidente em seus relatos a forma o obtidos ou seleciodivíduos, como se coletaram os dados, e prin, como se chegou às apresentadas.

Tipos de estudos

Os estudos cier características específicas no que tange ao sej tipo. De forma gera os podem ter caráter exploratório, descritivo, e ou preditivo. Expl er dizer que há novos aspectos, novos enfoé novas áreas a sere tas, podendo abrir campo para muitas e nova. Descritivo signific am feitos estudos exploratórios, permanece is com relação a cer hos ou sujeitos de pesquisa, os quais devem s. Explanatório signi er relações causa/efeito. Preditivo pretende - síveis cenários ou cias.

Os trabalhos oodem ter aplicação imediata, ou de form, nem mesmo se vilguma aplicação para o fenômeno observado resultado da pesc

Pode-se obser po de pesquisa depende do enfoque ou crit- dido pelo autor, bedecer a interesses em particular (ou a des condições). Pode ar os tipos de pesquisas de diversos modos e o quadro a segui

Contudo, obse não haver unanimidade em definir os critérios e caráter social enfas tipos, ao passo que nas Exatas notamos alg s às Ciências anteri ndo contudo outros específicos.

A seguir, realiz descrição dos tipos:

1 – Básica – pli ar o campo de conhecimento teórico – sem o preocupar-se com aplicabilidade dos resultados. Seus resultad er leis, princípios ou ções.

2 – Aplicada sultados que possam ser utilizados na solu- blemas reais [13]

3 – Descritiva - rever situações, eventos ou fenômenos. O estu o tem como requisi imento prévio considerável da área de estud e se possa formula as de pesquisa [19][13].

4 – Exploratório – procura examinar um tema ou área pouco estudado, ou sob um novo enfoque. Sua utilização é aumentar o grau de familiaridade com fenômenos ou eventos pouco conhecidos [19] [MAR90].

5 – Correlacional – busca estabelecer relações entre dois ou mais conceitos, ou o grau de relação entre esses conceitos. O principal objetivo é determinar como se comporta um conceito, na presença de outro. Bastante similar ao tipo "Explanatória", onde se busca estabelecer a relação causa-efeito enter os conceitos [19].

6 – Preditivos – procura predizer os resultados de um fenômeno, ou ainda, seus eventos e comportamentos.

De modo geral, os estudos podem iniciar com um tipo, mas não se situar em apenas um dos tipos. O pesquisador pode descobrir outros enfoques durante o trabalho de pesquisa. Pode ocorrer que pesquisadores pretendam conduzir uma pesquisa dentro de determinado enfoque e seja obrigado a direcionar para outro – por exemplo, um estudo inicialmente exploratório pode ser obrigado a redirecionar os esforços para um estudo descritivo, em vista de haver descoberto durante o processo de pesquisa que seu trabalho já teve precedentes.

Tipos de Métodos de Pesquisa

Classicamente, autores [19] [8] [13]dividem os métodos de pesquisa em sete tipos de métodos de pesquisa: a bibliográfica, o *survey*, a experimentação, o estudo de caso, a histórica, a pesquisa-ação.

Os quatro primeiros incorrem em uma postura menos participativa do pesquisador. Assim sendo, parte-se sempre do princípio de que há uma nítida separação entre o objeto a ser estudado e o pesquisador. Não é permitida nenhuma forma de interação entre os dois: isso incorreria em uma forma de parcialidade ou influência nos resultados da pesquisa, o que inviabilizaria o trabalho de pesquisa. Tem ampla influência positivista.

O quinto pode, por vezes, admitir a participação do pesquisador – embora não o seja possível no contexto temporal. Destaca-se que nem sempre o pesquisador, nesse método, assume uma postura distante do objeto – embora utilize, muitas vezes, artifícios que os métodos com influência positivista empregam. É, muitas vezes, dito seguir a abordagem do paradigma interpretativo.

O sexto pressupõe ampla participação – e até convivência – do pesquisador no problema. Parte-se do princípio que o pesquisador faz parte do contexto do problema de pesquisa, e assim sendo, deve ser citado no trabalho, com todas as informações per-

tinentes as suas intervenções. Por essa metodologia também a por intervenção. Diferente das outras, não se parte de hipóte pressupostos. É uma metodologia mda em pesquisa social – l, na Antropologia. Diz-se fazer parte dia crítico.

A Ciência da Computação, por se tra ciência muito recente, vai au agregando metodologias amplamente n outras Ciências – razão pe- mos observar diversas metodologias n como será descrito em seç.

A seção a seguir apresenta – na pte, um breve apanhado dis métodos de pesquisa empregados na xatas de forma tradiciona so de haver alguma diferença notável e ase da pesquisa – como, po, uma forma diferente de realizar a vali indicada no desenvolvim n. Posteriormente, são apresentados os e pesquisa que vêm se del o graças ao advento dos recursos com .

Diversas têm sido as variações e as apresentadas em artigos da Computação – de certa forma, bas as daquelas tratadas até a itz e Wallace [25], em artigo publicado propõem usar modelos eis para realizar uma atividade nem se nte nos artigos de event os da Computação: a validação. No mesa zem os autores algumas es constatações, as quais tentar-se-á ver desenvolvimento do pres o.

Embora voltado para a área de E le *Software* – e, de modo ral, para a experimentação –, há conceil em vir a ser aplicados na ia de pesquisa em geral. Um deles é o todo.

De acordo com Adrion [1], podem diferentes tipos de abord er:

- Método científico – cientis lvem uma teoria para m determinado fenômeno; eles prop hipótese(s), e então tes es da hipótese. Assim procedendo, e dados para verificar ou ar as afirmações da(s) hipótese(s).
- Método tecnológico – engen volvem e testam uma sol ma hipótese. Baseado nos resultados d quela solução é increme ue não seja mais necessária nenhuma
- Método empírico – um m tico é proposto como ara validar determinada hipótese. Dif método científico, pode um modelo formal ou alguma teoria va a hipótese. Os dados os para verificar a hipótese.

- Método analítico – uma teoria formal é desenvolvida, e os resultados derivados daquela teoria podem ser comparados com observações empíricas.

Já Zelkowitz [25] busca categorizar modelos de validação de trabalhos – citando diversos métodos de pesquisa, tais como o estudo de caso, simulação e outros –, em três categorias: observacionais, históricos e controlados. Pode-se verificar que, normalmente, os métodos de pesquisa podem ser classificados baseados na possibilidade ou não de serem replicados, e da possibilidade de se exercer um maior controle ou não. Zelkowitz agrega, em se tratando de desenvolvimento de *software*, dois aspectos: a influência – ou impacto – que um projeto terá em um produto final, ou em um experimento; e propriedades temporais – considerando que a coleta de dados, para o trabalho de pesquisa ou de desenvolvimento de *software* poderá ser histórica ou atual.

Jenkins [9] classifica os métodos conforme estudos na área específica de Sistemas de Informação. Em seu estudo, apresenta 13 métodos; apresenta-se a seguir aqueles métodos com maior vínculo com a Ciência da Computação, a saber:

A – Modelagem ou demonstração matemática: dentre os métodos, certamente é o mais formal, buscando modelar o mundo real, e apresentar os resultados como resultados de equações matemáticas. Jenkins define como um "sistema determinístico e fechado, na qual todas as variáveis – tanto as dependentes, quanto as independentes, são previamente conhecidas e consideradas no modelo". Observa-se, nesse método, que a intervenção não é possível.

B – Simulação experimental: método que usa um modelo fechado de simulação, para representar um segmento do mundo real. Aqui, os sujeitos humanos são expostos a esse modelo, e suas respostas são registradas. Jenkins coloca que "o pesquisador é quem determina o tempo e a natureza dos eventos experimentais.

C – Experimento de laboratório: é a experimentação tradicional, aqui destacando-se o uso de um ambiente de controle: o laboratório.

D – Simulação livre: método similar à simulação experimental, mas com a diferença de que o controle temporal e a natureza dos eventos não apenas são definidos pelo pesquisador, mas também pelo comportamento do objeto de pesquisa.

E – Experimento de campo: ao invés de ocorrer em um ambiente de total controle, o pesquisador usa o ambiente natural, "manipulando as variáveis independentes enquanto tenta controlar as mais importantes variáveis intervenientes, para então medir esses efeitos".

F – Experimento adaptativo: é o método de quase-experimento, que envolve medi-

ções antes e depois1ento, além de necessitar de um grupo de controle, para efetuar as compara2rnarão possíveis as medições.

G – Estudo de 1ilar ao experimento de campo, com a diferença que o pesquisador não ma1ariáveis independentes, mas unicamente as dependentes.

Os outros méto1ntados por Jenkins são o estudo de caso – conforme já tratado em capítul1 e métodos com uma enorme ênfase na pesquisa social, tais como Análise c1 de grupo, Pesquisa de opinião, Pesquisa ou observação participativa, Pesq1uivos e Pesquisa filosófica.

Um método bante e frequentemente utilizado no Brasil é chamado de "dissertação-proje1nte do avanço das áreas das Ciências Exatas e Tecnológicas, tendo sido 1ais como uma metodologia de pesquisa tecnológica do que científica. Sim1enção, busca identificar um problema dentro de alguma área, caracterizar 2senvolver uma solução para o problema. Muitas vezes, esse problema é 1 apenas conceitualmente. A solução é, na maior parte dos casos, uma i1ção de um programa de computador. Diferentemente da intervenção, o1não se identifica, em momento algum, a influência do pesquisador-dese1no objeto a ser desenvolvido – mas unicamente com o problema de pes1esolvido.

Considerações1re os métodos

A Ciência da C pode ainda ser considerada uma Ciência híbrida, uma vez que envolve 1cnicos – alguns com profunda fundamentação teórica, como Análise Con1, Criptografia ou teoria da Computação -, educacionais, e organizacionais, 6.

Por esse ângulealizar cuidadosa análise ao procurar identificar o método empregado em u1 outra publicação de caráter científico. Por exemplo, pode ser necessário ide1s foram as condições nas quais aquelas informações foram proferidas; da me se é possível efetuar repetições dos procedimentos ou não; o quão imparcial1isador; qual é a experiência do pesquisador; como foram realizadas as aná1ipóteses foram feitas; se é um primeiro estudo.

O estudo rea

O método em a pesquisa *survey*, cujo instrumento foram os próprios anais de eventos. Para dos temas componentes da sub-área escolhida – Segurança

Computacional –, iniciamos um estudo bibliométrico sobre fontes bibliográficas altamente relevantes, identificando os temas através das palavras-chave encontradas nessas fontes.

Sobre anais de Congressos, Simpósios, *Workshops* e Encontros (principalmente, CRYPTO, EUROCRYPT, SAFECOMP, IFIP/SEC e ICICS) cujos temas tratavam sobre essas palavras-chave, iniciamos o processo de análise, identificando – no corpo dos artigos – características que identifiquem os métodos de pesquisa que foram utilizados para que se pudessem ser feitas as afirmações ou conclusões de pesquisa. Posteriormente, passou-se a montar os tópicos de interesse – as variáveis – em uma planilha eletrônica. Todos os eventos encontrados foram analisados e catalogados. Em algumas situações, no caso de ocorrência de propor algo, ou idéia inovadora, foi colocado como "Proposta de Conceito". As variáveis de interesse foram: dados identificatórios do artigo e do(s) autor(es), ano de publicação, evento, tema de pesquisa, tipo de método empregado, se esse método está explícito ou não, caráter da pesquisa, instituição e país de origem. Na prática, as principais variáveis compõe escalas do tipo nominal – o que limitou bastante o tipo de análises possíveis de serem realizadas. Ainda assim, foi possível, através de recursos de filtragem, realizar algumas análises.

Assim sendo, os métodos que se esperavam poderem aparecer são os indicados no quadro a seguir.

Método de pesquisa
Demonstração matemática
Dissertação-Projeto
Estudo comparativo
Estudo de campo
Estudo de caso
Experimentação
Histórica
Proposta de Conceito
Simulação
Survey

Quadro 1: Métodos de pesquisa esperados

Fonte: Elaborado pelo autor.

Tabela 1: Percentuais encontrados

Tipo de Método	% encontrado
Proposta de Conceito	42,33
Demonstração Matemática	42,22
Experimentação	5,04
Dissertação-Projeto	3,99
Estudo Comparativo	2,31
Estudo de Caso	1,05
Survey	0,52
Simulação	0,42
Não definido	0,31
Definição de Protocolo	0,31
Histórica	0,31
Bibliográfico	0,21

Fonte: Elaborado pelo autor

Com relação aos temas de pesquisa, os mesmos foram armazenados, resulta 97 temas ou áreas de interesse, dentro da Criptografia – tendo muitos itens em com Segurança Computacional.

Resultados obtidos

Lembra-se que toda e qualquer informação afirmada no corpo do presente refere-se ao universo definido – ou seja, métodos utilizados em artigos publica eventos internacionais da área de Segurança Computacional, com ênfase em Cript Como em qualquer estudo realizado onde se utiliza a pesquisa *survey*, a gener. é possível, dentro de determinadas condições, e apenas para o universo conside

A seguir, apresentamos os resultados da pesquisa univariada sobre algumas d. veis definidas anteriormente. As variáveis que eram de interesse para o presente t eram o tipo de método empregado no artigo, o país onde a pesquisa foi real Instituição de pesquisa, o caráter da pesquisa, os temas mais pesquisados, e se o de pesquisa era expresso de forma explícita, seja no *abstract*, seja no corpo do a

Conforme se pode observar no gráfico da figura acima, os tipos preponder. metodologias que observamos são a Proposta de Conceito, seguido da Demor Matemática, da Experimentação e da Dissertação-Projeto. No caso dos dado analisados, o termo "indefinida" se refere ao fato de não apenas não se enqua

nenhuma das outras metodologias, mas também pelo fato de que esses artigos não traziam contribuição científica, mas meramente opiniões.

Com relação aos países de origem, observamos algumas especiais considerações. Como o intervalo temporal da coleta dos dados referia-se a artigos desde o início dos anos 80, ocorreram algumas alterações na Geografia política mundial. Assim, embora alguns artigos se referissem a países como "União Soviética", "Iugoslávia", "Checoslová-quia", "Alemanha Ocidental", "Alemanha Oriental", optou-se por adaptar à realidade vigente na época do presente trabalho – primeiro semestre do ano 2000.

Sendo assim destaca-se, na tabela a seguir, os 15 países com maior produção na área de Pesquisa em Segurança Computacional, apresentados na tabela a seguir, por ordem decrescente.

Tabela 2: Produção por país de origem

Países	% Ocorrências
Estados Unidos	24
Austrália	10
Reino Unido	9
Alemanha	9
França	8
Japão	7
Suíça	3
Canadá	3
Bélgica	3
Israel	3

Fonte: Elaborado pelo autor, com base na pesquisa realizada.

Observa-se que a produção desses 10 países, dentre os 31 observados, representa 79% do total. Embora não apresentado acima, houve 15 artigos onde não foi explicitada a origem, nem foi possível identificar por intermédio da origem de seus autores ou Institui-ções de Pesquisa – por se tratar de autor único, e/ou não citar a Instituição de Pesquisa.

Com relação ao caráter da pesquisa, constatou-se um predomínio nos caráteres Descritivo (55,15%) e Exploratório (43,91%). Pequenas ocorrências observadas em artigos com caráter explanatório – causa/efeito, ou origem/consequência. Alguns artigos não puderam ter o seu caráter identificado. Já com relação à forma de apresentar o trabalho, observa-se que maior parte da forma de apresentar a metodologia é explicita (52,52%) –

normalmente, no resumo. Para o restante, identificamos como realmente foras procedimentos que permitiam chegar a conclusões pela leitura do corpo dos foram consideradas como a forma "implícita" de apresentar a metodologia.

A seguir, apresentam-se os resultados obtidos com relação à produ autores – cita-se os quinze autores de maior produtividade e instituições.

Tabela 3: Os quinze autores mais produtivos

Autores mais produtivos	% ocorrências
MOTI YUNG	1,17
REIHANEH SAFAVI-NAINI	0,95
ED DAWSON	0,78
ROSS ANDERSON	0,73
BRUCE SCHNEIER	0,67
JACQUES STERN	0,67
JOVAN DJ. GOLIC	0,67
KOUICHI SAKURAI	0,61
TATSUAKI OKAMOTO	0,56
YULIANG ZHENG	0,56
COLIN BOYD	0,50
DAVID WAGNER	0,50
JOHN KELSEY	0,50
MIHIR BELLARE	0,50
YAIR FRANKEL	0,50

Fonte: Elaborado pelo autor, com base na pesquisa efetuada.

Tabela 4: As quinze instituições mais produtivas

Instituições mais produtivas	% ocorrências
Queensland University of Technology	4,31
University of California	2,42
University of Wollongong	1,79
Katholieke Universiteit Leuven	1,68
MIT	1,47
University of London	1,37
Não declarada no do artigo	1,16
École Normale Superieure	1,16
Counterpane Systems	1,05
NTT Laboratories	1,05

AT&T LABS	0,95
University of Cambridge	0,95
Weizmann Institute	0,95
IBM T. J. Watson Research Center	0,84
Monash University	0,84

Fonte: Elaborado pelo autor, com base na pesquisa realizada.

A soma da produção desses autores é de quase 10 % da produção total. O número total de autores foi de 1792 pessoas. Um fato a ser destacado é a relação entre o número de pesquisadores e o número de artigos, o que resultou em uma razão de 1.88 pesquisadores por artigo. Em análise a ser apresentada posteriormente, observa-se que esse quadro está se modificando com o tempo – os artigos iniciais eram produções individuais, ao passo que atualmente nota-se a produção em equipes, mesmo encontrando-se em áreas geográficas distantes.

Uma das questões de interesse no trabalho era a identificação de quais são as instituições de pesquisa ou de ensino que têm apresentado maior produção científica. Essa informação pode denotar um interesse mais profundo – provavelmente, um grupo de pesquisa, caso mais de um autor tenha trabalhado esses temas, na mesma instituição – , ou mesmo a existência de um projeto de maior vulto do que publicações isoladas – identificado pela continuidade temporal da produção sobre o mesmo tema. A produção dessas instituições chega a aproximadamente 26 % da produção total pesquisada. Entre as cinco primeiras, duas são australianas, duas americanas e uma belga. Há autores que não citam informação alguma referente à instituição de origem – seja de ensino, seja de pesquisa ou mesmo comercial. Assim, foram agrupadas no item "Não declarada no corpo/resumo do artigo" – e corresponderam a um número total de ocorrências maior do que o número de ocorrências de algumas instituições de renome, tais como Weizmann Institute, Cambridge University, Siemens ou mesmo IBM. Uma informação de interesse é o fato de haver diversas instituições não acadêmicas, o que revela o interesse, a seriedade, e a preocupação comerciais do assunto de pesquisa – a Segurança Computacional (Criptografia).

O agrupamento de temas dos anais desses eventos totalizaram 97 temas, tendo ocorrido temas desde "agentes" até "vulnerabilidade", em ordem alfabética. Os temas dos primeiros trabalhos referiam-se, principalmente, a "esquemas de cifragem", tendo ocorrido outros mais recentemente – tais como "agentes", ou "dinheiro digital".

Esses quinze temas foram responsáveis por cerca de 48 % do total da ia pesquisa realizada. Observamos que há uma contribuição elevada de aspas relacionados à criptografia, por haver um maior número de eventos dem colhidos os artigos – que consiste a maior parte da bibliografia encontrais de eventos na Biblioteca do Instituto de Informática da UFRGS.

A seguir, apresenta-se os temas de maior frequência de aparecimento

Tabela 5: Temas com maior ocorrência

Tema do artigo/pesquisa	% Ocorrências
Criptoanálise	5,15
Dinheiro digital	5,04
Cifras	4,73
Assinaturas digitais	4,31
Chave pública	3,99
Protocolos	3,78
Autenticação	3,26
Ataques/invasão	2,84
Criptografia	2,73
Segurança em redes	2,73
Controle de acesso	2,10
Compartilhamento de segredo	2,00
Comércio eletrônico	1,89
Complexidade	1,68
Curvas elípticas	1,58

Fonte: Elaborado pelo autor, com base na pesquisa realizada.

Limitações do estudo, considerações finais e perspectivas

A presente seção apresenta as dificuldades e considerações tomadas, nclusões e sugestões para desenvolvimento de trabalhos futuros.

Dentre as dificuldades encontradas, podemos destacar problemas co os anais dos eventos – e com os sujeitos de pesquisa. Ademais, a própria gia *survey* é orientada para enquetes e questionários, os quais têm – de –, diversos tipos de variáveis. As variáveis aqui definidas eram de escala que limita o tipo de testes estatísticos possíveis de serem realizados. O processar a análise, utilizando-se da análise multivariada, ficou restrita ao uso e análas de dados estratificados e/ou agrupados pelos mais diversos critérios.

Ademais, a bibliografia empregada – a qual continha o substrato para os sujeitos de pesquisa – foi muito concentrada em uma área específica: a Criptografia. Ademais, as edições que foram empregadas ficaram limitadas aos exemplares de 37 eventos ocorridos em diversos anos, em diversos locais. Houve uma concentração de exemplares dos últimos sete anos – havendo alguns exemplares com mais de 15 anos, nos quais se observa uma grande diferença nos enfoques nos quais se trabalhavam os conceitos de Criptografia, e mesmo na forma de escrita dos artigos

Uma das questões indiretas de interesse era o quão recentes eram os artigos utilizados em referências bibliográficas nos artigos que foram sujeitos de pesquisa. Essa questão poderia indicar, por exemplo, se um tema se baseia principalmente em artigos clássicos, ou se estaria aberto a novas idéias e temas. Para tanto, foi acrescentada uma coluna na planilha eletrônica, com o título ano da referência mais recente. Houve grande dificuldade em preencher essa coluna, uma vez que para referências de características semelhantes, os pesquisadores referenciavam de modo diferente. Isso ocorre provavelmente porque a forma de referenciar, na Ciência da Computação, é diferente de todas as outras Ciências. A mesma referência pode ser vista diferentemente em artigos diversos, conforme o exemplo abaixo:

SAMPIERI, Roberto Hernández, COLLADO, Carlos Fernández, e LUCIO, Pilar Baptista. **Metodología de la Investigación.** México: McGraw-Hill, 1991. 514 p.

ou

[19] SAMPIERI, Roberto Hernández, COLLADO, Carlos Fernández, e LUCIO, Pilar Baptista. **Metodología de la Investigación.** México: McGraw-Hill, 1991. 514 p.

Essas formas diferentes, em um artigo com muitas referências, dificultam a identificação da referência mais recente. Destacamos que a primeira forma é a mais utilizadas em outras Ciências, sendo a segunda tradicionalmente utilizada – unicamente – em Ciência da Computação. Basicamente, pode-se identificar se um pesquisador é ou não da área pela forma de referenciar um artigo.

Uma observação interessante é que, em diversos artigos recentes, têm-se utilizado uma forma diferente de referência a múltiplos autores, conforme vê-se no exemplo abaixo:

[SCL 91] SAMPIERI, Roberto Hernández, COLLADO, Carlos Fernández, e LUCIO, Pilar Baptista. **Metodología de la Investigación.** México: McGraw-Hill, 1991. 514 p.

Observa-se que o indicador inicial apresenta as iniciais de cada um dos três autores, ao invés das três letras iniciais do último sobrenome. A tendência observada em publicações pela IEEE é a seguinte:

[33] SAMPIERI, Roberto Hernández, Carlos Fernández, e LUCIO, Pil
tista. **Metodología de la Investigación.**cGraw-Hill, 1991. 514 p.

Sendo a trigésima terceira referência no artigo em questão.

Segurança computacional – em espotografia – ainda apresenta
dades, graças à grande diversidade de e de conhecimento. Por e
há casos de temas de Criptografia emaliza pesquisa estritamente
– como demonstrar matematicamentções de uma pesquisa env
criptografia –, e também experimens, em ambiente real – co
protocolo criptográfico para garantir ade de em remetente de um
bancária. Em ambos os casos, está senco um trabalho de pesquisa -
de formas, conteúdos e objetivos difer

Além disso, se considerarmos a áreSegurança Computacional,
observar quebras de paradigmas realizalocidade surpreendentemer
mica – podemos citar o caso de vírus de or, os quais sempre se caracte
por limitar-se a apenas uma plataformou Mac) e, posteriormente,
de macro vieram a mudar essa afirmao da Criptografia, têm-se ob
grande ênfase para tópicos como curs, criptografia quântica, crip
biométrica e alguns protocolos criptogsiderados esotéricos [20].

Outra dificuldade diz respeita aos mpregados: há, mesmo na li
especializada, alguma confusão no qu iversos termos. O mais crític
a expressão "metodologia" – que seria os métodos das Ciências -, c
todo" – modo ou forma de proceder, p a um fim.

Ainda há pouca definição em especihétodos de pesquisa na área e
Walter F. Tichy [22] realizou uma pesqubre 400 artigos que afirmav
realizado experimentação; grande pagos (40 %) havia realizado "
empírica", com nenhum suporte cients artigos foram excluídos da
a ser analisada, em razão de se apoias em demonstração maten
teoremas – o que não pode ser provaerimentos. Já Marvin Zelko
realizou outra pesquisa por enquetes, o 600 artigos publicados – te
apresentados como "foi aplicado expeo" –, tendo observado que
não validava experimentação especifidologia, e mesmo nenhum
autores utilizaram conceitos de valida do de caso; e a terminologia
rimentação era, na maioria dos casos, . Destaca ainda que, aparen
o número de artigos sem validação pantar.

Pouca surpresa ocorreu, ao agruparmos os temas de pesquisa por métodos, ou mesmo por países. No caso do agrupamento de temas por países, há a supremacia norte-americana em praticamente todos os temas de pesquisa. Já no caso de agrupamento de temas por métodos, os métodos mais formais foram observados em temas de pesquisa que realmente requeriam formalidade matemática; da mesma forma, métodos experimentais foram observados em temas recentes, os quais necessitam compor um corpo de conhecimento – ou seja, exatamente onde era necessário um estudo exploratório.

É relevante destacar o método de pesquisa, ao se escrever um artigo referente a um trabalho de pesquisa na área de Segurança Computacional? Aparentemente, sim. Qualquer produção onde se coloque de forma explícita o método utilizado permitirá que outros cientistas da Computação repliquem o estudo, ou que, pelo menos, tenham uma melhor condição de avaliar o processo de desenvolvimento e os resultados do estudo, bem como a sua qualidade.

Um aspecto que poderia vir a incrementar a qualidade do presente estudo seria o uso de outras formas de validação. Mesmo no caso da dissertação-projeto, metodologia que tem-se destacado – amplamente utilizada em países onde a Ciência da Computação é mais recente –, deve-se usar alguma forma de validação do trabalho efetuado, bem como explicitar todas as fases do estudo realizado. Por exemplo, Zelkowitz [25] propõe diversos métodos para efetuar validação – embora mais dirigido a experimentações –, entre os quais buscou classificar nas categorias a seguir:

- observacional – os métodos observacionais coletam dados relevantes, da mesma forma que desenvolvimento de um projeto – há pouco controle sobre o desenvolvimento de projetos inovadores;
- histórico – a coleta de dados ocorre sobre projetos já completados, tal como em um projeto baseado em engenharia reversa – o dado já existe, sendo necessário apenas a sua análise; e
- controlado – usa múltiplas instâncias de uma observação para validação estatística dos resultados – onde se pode empregar, por exemplo, uma simulação.

O presente estudo utilizou-se apenas da validação aparente – confiando à experiência de especialistas. Porém, dadas as escalas de nosso estudo, análises formais não seriam de possível realização, e não seria possível uso de técnicas de pré ou pós testagem, em função de não existir instrumento para avaliação – questionários –, o qual poderia conter viéses ou erros.

Certamente, para a realização de trabalhos futuros, deve-se aumentar trabalhada – ou seja, analisar um número maior de artigos, sendo a situação car a TODOS os eventos da área de interesse, de TODOS os anos em que ess ocorreram. É interessante não apenas certificar-se de cobrir todos os even mas também de todas as áreas da segurança computacional. O fato de n essa aleatoriedade implica a citação dessa fraqueza, em cada afirmação conclusões no trabalho presente.

Um trabalho que certamente seria frutífero é a formalização do métod dissertação–projeto. Há a necessidade de formalizar formas de obtenção procedimentos de trabalho e, principalmente, validação do mesmo. Essa m tante usado no Brasil, tem aplicabilidade em toda a Ciência da Computaçã âmbito desse estudo transcende um trabalho individual vindo a constituir, um trabalho de doutorado.

Dados e análises completos do trabalho encontram-se disponíveis na área de download da página em www.sinpro-rs.org.br/vinicius.gadis.ribei "TI1 – Métodos de Pesquisa empregados em Segurança Computacional – C

Bibliografia

[1] ADRION, W. R. **Research Methodology in Software Engineering:** Sum Dagstuhl Workshop on Future Directions in Software Engineering. SIGSoft S Notes. New York, ACM Press: v. 18, n.1, p. 36-37, 1993.

[2] BABBIE, Earl. **Survey Research Methods.** 2. ed. Belmont: Wadsworth:

[3] BENBASAT, I., MOORE, G. Development of Measures for Studying Emerg gies. In: HAWAII INTERNATIONAL CONFERENCE ON SYSTEMS SCIENCES (HICS Proceedings... Los Alamos: IEEE Society Press, p. 315-324.

[4] BRYMAN, Alan; BURGESS, Robert. **Analyzing Quantitative Data.** Londo 1995. 236 p.

[5] FINK, Arlene. **How to analyze survey data.** Thousand Oaks: Sage, 19 The Survey Kit. il.

[6] FINK, Arlene. **The survey handbook.** Thousand Oaks: Sage, 1995. v Survey Kit. il.

[7] GIL, Antônio C. **Como elaborar projetos de pesquisa.** 3. ed. São Paul 159 p. il.

[8] HOPPEN, Norberto; LAPOINTE, Liette; MOREAU, Eliane. **Um Guia para de**

Artigos de Pesquisa em Sistemas de Informação. Porto Alegre: PPGA-UFRGS, 1996. 18 p. Série Documentos para estudo. Disponível na Internet. http://www.cesup.ufrgs.br/PPGA/read/artigo/guia a.htm 08nov 96

[9] JENKINS, A. Milton. **Research methodologies and MIS research.** Research methods in information systems. Amsterdam: North-Holland, 1985. 320 p. Trabalho apresentado no IFIP WG8.2 Colloquium, 1984, Manchester. il.

[10] KERLINGER. Fred N. **Metodologia da Pesquisa em Ciências Sociais:** um Tratamento Conceitual. São Paulo: EPU, 1980. 386 p. il.

[11] KNIGHT, John C.; LEVENSON, Nancy G. **An experimental Evaluation of the Assumption of Independence in Multiversion Programming.** IEEE Trans. Software Eng., New York, p. 96-109, Jan 1986.

[12] LITWIN, Mark S. **How to measure survey reliability and validity.** The Survey Kit, no.7. Thousand Oaks: Sage, 1995. 90 p.

[13] MARCONI, Marina de Andrade, e LAKATOS, Eva Maria. **Técnicas de Pesquisa.** 2. ed. São Paulo: Atlas, 1990. 234 p. il.

[14] MATTAR, N. **Pesquisa de Marketing.** 3. ed. São Paulo: Atlas, 1996. v.2. 248 p. il.

[15] ORLIKOWSKI, W., BAROUDI, J. **Studying Information Technology in Organizations:** Research Approaches and Assumptions. Information Systems Research. New York, v.2, n.1, p. 1-28, Aug. 1991.

[16] PETER, P. J. **Construct Validity:** A Review of Basic Issues and Marketing Practices. Journal of Marketing Research. p. 6-17. May 1981.

[17] PINSONNEAULT, A.; KRAEMER, K. **Survey Research in Management Information Systems:** An Assessment. Journal of Management Information Systems. New York, v.10 n. 2, p. 75-106, Fall 1993.

[18] RIBEIRO, Vinicius G. **Um estudo sobre os métodos de pesquisa utilizados em Segurança Computacional.** Porto Alegre: PPGC da UFRGS, 2000. 70 p. TI 916. Disponível na Internet em <http://www.sinpro-rs.org.br/vinicius.gadis.ribeiro>

[19] SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, Pilar Baptista. **Metodología de la Investigación.** México: McGraw-Hill, 1991. 514 p. il.

[20] SCHNEIER, Bruce. **Applied Cryptography.** New York: John Wiley & Sons, 1995. 624 p. il.

[21] STRAUB, D. **Validating research instruments.** MIS Quarterly. Minneapolis, v. 13, n.3, p. 147-169, Jun 1989.

[22] TICHY, Walter et al. **Experimental Evaliation in Computer Science:** A Quantitative

Study. J. Systems and Software, New York, p. 1-18, Jan. 1995.

[23] TICHY, Walter F. **Should computer scientists experiment m**omputer. New York, v. 15, n. 3,. p. 32-40, May 1998. il.

[24] YIN, Robert K. **Case study research:** design and methods.2on: Sage, 1994. 174 p. il.

[25] ZELKOWITZ, Marvin V.; WALLACE, Dolores R. **Experimental m**alidating **technology.** IEEE Computer. New York, v. 15, n. 3, p. 23-31, May 1

ANEXO 5
UM EXEMPLO DE INTERVENÇÃO

Nesse exemplo, é interessante observar a descrição da organização, do problema, a técnica de modelagem (computacional), a implementação da solução e a discussão de resultados. O artigo em questão foi apresentado no WorkShop de Segurança em Sistemas Computacionais – Wseg 2001.